Invariant Theory (Humphreys Chap. 3)

It's a classical topic.

We'll focus on finite groups $G \subset GL_n(\mathbb{C}) = GL(V)$

$V = \mathbb{C}^n$

$\mathbb{C}$-basis $e_1, \ldots, e_n$

as they act on $\mathbb{C}[\underbrace{x_1, \ldots, x_n}_{\text{a } \mathbb{C}\text{-basis for } V^*}] =: \mathbb{C}[\underline{x}]$ polynomial ring

via linear substitutions:

$$\text{for } g \in G, \quad g(f(\underline{x})) := f(g^{-1}\underline{x}).$$

Want to study, describe the G-invariant subring

$$\mathbb{C}[\underline{x}]^G := \{ f(\underline{x}) \in \mathbb{C}[\underline{x}] : g(f(\underline{x})) = f(\underline{x}) \ \forall g \in G \}$$

EXAMPLES

(1) $G = \mathfrak{S}_n$ acts on $\mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[\underline{x}]$ by permuting variables, and

THEOREM: $\mathbb{C}[\underline{x}]^{\mathfrak{S}_n} = \mathbb{C}[e_1, e_2, \ldots, e_n]$

(Fundamental Thm of Symmetric Functions)

$e_1 = x_1 + x_2 + \cdots + x_n$, $e_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$, $e_n = x_1x_2\cdots x_n$

sketch proof: $\mathbb{C}[\underline{x}] = \bigoplus_{d=0}^{\infty} \mathbb{C}[\underline{x}]_d = \mathbb{C} \oplus \mathbb{C}[\underline{x}]_1 \oplus \mathbb{C}[\underline{x}]_2 \oplus \cdots$

$$\cup$$

$$\mathbb{C}[\underline{x}]^{\mathfrak{S}_n} = \bigoplus_{d=0}^{\infty} \underbrace{\mathbb{C}[\underline{x}]_d^{\mathfrak{S}_n}}$$

has a $\mathbb{C}$-basis of monomial symmetric functions $\{m_\lambda(\underline{x})\}_{\lambda \text{ a partition of } d}$

$(\lambda_1, \ldots, \lambda_n)$
$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$

e.g. $d=3$

$m_{111} = x_1x_2x_3 + x_1x_2x_4 + \cdots$

$m_{21} = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + \cdots$

$m_3 = x_1^3 + x_2^3 + \cdots$

There's a unitriangular change-of-basis in $\mathbb{C}[\underline{x}]_d^{\mathfrak{S}_n}$ to $\{e_\lambda(\underline{x}) := e_{\lambda_1} e_{\lambda_2} \cdots\}_{\lambda \text{ a partition of } d \text{ with all } \lambda_i \leq n}$

e.g.

$$\begin{array}{cc} & \begin{array}{ccc} e_{111} = e_1e_1e_1 & e_{21} = e_2e_1 & e_3 \\ = (x_1+x_2+\cdots)^3 & = (x_1x_2+x_1x_3+\cdots)(x_1+x_2+\cdots) & = x_1x_2x_3+x_1x_2x_4+\cdots \end{array} \\ \begin{array}{c} m_{111} \\ m_{21} \\ m_3 \end{array} & \begin{bmatrix} 6 & 3 & 1 \\ 3 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

This shows $\mathbb{C}[\underline{x}]^{\mathfrak{S}_n} = \mathbb{C}[e_1, \ldots, e_n]$ ▨

(2) Similarly, not too hard to show

$$G(d,1,n) = \left\{ \begin{array}{l} n \times n \text{ monomial} \\ \text{matrices with} \\ \text{nonzero entries in } \sqrt[d]{1} \end{array} \right\} \subset GL_n(\mathbb{C})$$

$d=1$: $\mathfrak{S}_n$ $d=2$: B_n/C_n

has $\mathbb{C}[\underline{x}]^{G(d,1,n)}$

$$= \mathbb{C}[\underbrace{e_1(x_1^d,\ldots,x_n^d)}_{= x_1^d + \cdots + x_n^d}, e_2(x_1^d,\ldots,x_n^d), \ldots, \underbrace{e_n(x_1^d,\ldots,x_n^d)}_{= x_1^d \cdots x_n^d = (x_1 \cdots x_n)^d}]$$

and

$$G(d,e,n) = \left\{ \begin{array}{l} g \in G(d,1,n) \text{ with} \\ \text{product of nonzero} \\ \text{entries in } \sqrt[d/e]{1} \end{array} \right\}$$

$e \mid d$

$d=e=2$: D_n $d=e=m$, $n=2$: $I_2(m)$

has $\mathbb{C}[\underline{x}]^{G(d,e,n)}$

$$= \mathbb{C}[e_1(\underline{x}^d), e_2(\underline{x}^d), \ldots, e_{n-1}(\underline{x}^d), (x_1 x_2 \cdots x_n)^{d/e}]$$

So all of the ∞ family of complex refl'n groups G

have $\mathbb{C}[\underline{x}]^W = \mathbb{C}[f_1,\ldots,f_n]$

with $f_1,\ldots,f_n$ homogeneous,

algebraically independent

(3) $$G = \Big\langle \underbrace{\begin{array}{c|cc} & e_1 & e_2 \\ \hline e_1 & -1 & 0 \\ e_2 & 0 & -1 \end{array}}_{g :=} \Big\rangle \cong \mathbb{Z}/2\mathbb{Z} \qquad \begin{array}{c|cc} & x_1 & x_2 \\ \hline x_1 & -1 & 0 \\ x_2 & 0 & -1 \end{array}$$

acting on $\mathbb{C}[\underline{x}] = \mathbb{C}[x_1, x_2]$ via $g(x_1) = -x_1$, $g(x_2) = -x_2$

has $\mathbb{C}[x_1,x_2]^G = \mathrm{span}_{\mathbb{C}}\{x_1^{a_1}x_2^{a_2} : a_1 + a_2 \equiv 0 \bmod 2\}$

$$= \underbrace{\mathbb{C}[x_1^2, x_2^2, x_1x_2]}_{\mathbb{C}\text{-subalg. gen'd by } \underbrace{x_1^2,\, x_2^2,\, x_1x_2}_{\text{not algebraically independent: } x_1^2 \cdot x_2^2 - (x_1x_2)^2 = 0}} \subset \mathbb{C}[x_1, x_2]$$

$$\begin{tikzcd} x_1^2 & x_2^2 & x_1x_2 & \mathbb{C}[x_1,x_2]^G \\ A \arrow[u, mapsto] & B \arrow[u, mapsto] & C \arrow[u, mapsto] & \mathbb{C}[A,B,C]/(AB - C^2) \arrow[u, "\wr"'] \end{tikzcd}$$

PROPOSITION: For any finite group $G \subset GL_n(\mathbb{C})$, $\mathbb{C}[\underline{x}]^G$ is at least finitely gen'd as an algebra over $\mathbb{C}$ by any $f_1, f_2, \ldots, f_m$ in $\mathbb{C}[\underline{x}]^G$ generating the Hilbert ideal $I := (\underbrace{\mathbb{C}[\underline{x}]^G_+}_{\mathbb{C}[\underline{x}]^G_1 \oplus \mathbb{C}[\underline{x}]^G_2 \oplus \cdots}) \subset \mathbb{C}[\underline{x}]$

The proof is easy, and uses an important recurring idea we've seen: averageing over G

DEF'N: In any finite-dim'l G-rep'n $\mathcal{U}$ over $\mathbb{C}$, the averaging/Reynolds operator

$$\begin{aligned} \mathcal{U} &\xrightarrow{\pi_G} \mathcal{U} \\ u &\longmapsto \pi_G(u) := \frac{1}{|G|} \sum_{g \in G} g(u) \end{aligned}$$

is an idempotent projection onto the G-fixed space $\mathcal{U}^G$.
$\pi_G^2 = \pi_G$

It still makes sense acting $\mathbb{C}[\underline{x}] \xrightarrow{\pi_G} \mathbb{C}[\underline{x}]$ (since each $\mathbb{C}[\underline{x}]_d$ is finite-dim'l), and it is $\mathbb{C}[\underline{x}]^G$-linear there: if $f \in \mathbb{C}[\underline{x}]^G$, $h \in \mathbb{C}[\underline{x}]$ then $\pi_G(fh) = \pi_G(f)\,\pi_G(h) = f \cdot \pi_G(h)$.

---

proof of PROP: Show every homogeneous $f \in \mathbb{C}[\underline{x}]^G_d$ lies in the $\mathbb{C}$-subalgebra gen'd by $f_1, \ldots, f_m$ via induction on d.

BASE CASE $d=0$. Then $\mathbb{C}[\underline{x}]^G_0 = \mathbb{C}$, so done.

INDUCTIVE STEP $d \geq 1$.

Since $f \in \mathbb{C}[\underline{x}]^G_d \subset I = (\mathbb{C}[\underline{x}]^G_+) = (f_1, f_2, \ldots, f_m)$

can write $f = \sum_{i=1}^m f_i h_i$ where $h_i \in \mathbb{C}[\underline{x}]_{d-\deg(f_i)}$

apply π_G

$$f = \pi_G(f) = \sum_{i=1}^m \pi_G(f_i h_i) = \sum_{i=1}^m f_i \, \pi_G(h_i)$$

lies in $\mathbb{C}[\underline{x}]^G_{d-\deg(f_i)}$,

so already in the subalgebra gen'd by $f_1, \ldots, f_m$

by induction

$\Longrightarrow$ f lies in this subalgebra. ■

PROPOSITION: The number m of G-algebra generators $f_1, \ldots, f_m$ for $\mathbb{C}[\underline{x}]^G$ satisfies $m \geq n$, with equality $\Longleftrightarrow$ they're alg. independent,

so $\mathbb{C}[\underline{x}]^G \cong \mathbb{C}[f_1, \ldots, f_n]$

a polynomial ring.

To prove this, either one uses ring theory of Krull dimension and integral ring extensions, or some field theory ideas...

DEFIN: For a field extension $K \subset L$, the transcendence degree of L over K

$$\operatorname{trdeg}_K(L) := \max\{n : \exists\, \alpha_1, \ldots, \alpha_n \in L \text{ alg. independent over } K\}$$

= n appearing in any field tower of this form:

$$\begin{array}{ccc} L & & \\ \Big| \text{ algebraic} & & \text{rational functions} \\ K(\alpha_1, \ldots, \alpha_n) & \cong & K(x_1, \ldots, x_n) \\ \Big| \text{ purely transcendental} & & \\ K & & \end{array}$$

Call any such $\alpha_1, \ldots, \alpha_n \in L$ a transcendence basis for L over K.

EXAMPLE

$$\begin{array}{ccc} K & \subset & L \\ \| & & \| \\ \mathbb{Q} & & \mathbb{Q}(\sqrt[6]{\pi}, x, y, \sqrt{2}) \end{array}$$

has $\operatorname{trdeg}_K(L) = 3$, with some transcendence bases

$\{\pi^5, x, y\}$, $\{\sqrt{\pi}, x^2 + \pi, y^{10} - x^4\}$, ...

---

proof of PROP: It's enough to show that $\{f_1, \ldots, f_m\}$ contains a transcendence basis for $\underset{= \mathbb{C}(\underline{x})}{L = \mathbb{C}(x_1, \ldots, x_n)}$ over $\underset{K}{\overset{\|}{\mathbb{C}}}$, since $\operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(\underline{x}) = n$.

$\{f_1, \dots, f_m\}$ generating $\mathbb{C}[\underline{x}]^G$ as a $\mathbb{C}$-algebra

$\Rightarrow \underbrace{\mathrm{Frac}}\left(\mathbb{C}[\underline{x}]^G\right) = \mathbb{C}(f_1, f_2, \dots, f_m)$ as a field extension $/\mathbb{C}$

field of fractions $:= \left\{ \frac{p(\underline{x})}{q(\underline{x})} : p, q \in \mathbb{C}[\underline{x}]^G,\ q \neq 0 \right\}$

But the inclusion $\mathrm{Frac}\left(\mathbb{C}[\underline{x}]^G\right) \subseteq \mathbb{C}(\underline{x})^G$ is actually an equality:

given $\frac{p(\underline{x})}{q(\underline{x})} \in \mathbb{C}(\underline{x})^G$, rewrite it as

$$\frac{p(\underline{x}) \cdot \prod_{\substack{g \in G \\ g \neq 1}} g(q(\underline{x}))}{q(\underline{x}) \cdot \prod_{\substack{g \in G \\ g \neq 1}} g(q(\underline{x}))} \in \mathrm{Frac}\left(\mathbb{C}[\underline{x}]^G\right)$$

denominator is G-invariant, hence so is numerator

Also the field extension $\mathbb{C}(\underline{x})^G \subset \mathbb{C}(\underline{x})$ is a finite algebraic Galois extension with Galois group G (by Galois Theory).

Hence we have

$$\left.\begin{array}{c} \mathbb{C}(\underline{x}) = \mathbb{C}(x_1, \dots, x_n) \\ \Big| \text{ algebraic} \\ \mathbb{C}(\underline{x})^G = \mathbb{C}(f_1, \dots, f_m) \\ \Big| \\ \mathbb{C} \end{array}\right\}$$

$\Rightarrow f_1, \dots, f_m$ contains a transcendence basis for $\mathbb{C}(\underline{x})$ over $\mathbb{C}$, so $m \geq n$ and equality $\Rightarrow$ alg. independence $\blacksquare$

One reason Shephard & Todd produced their 1955 classification of complex ref'n groups $G \subset GL(V)$, $V=\mathbb{C}^n$ acting irreducibly ($= G(d,e,n)$ + 34 exceptional groups) was to prove the backward implication here.

(Shephard-Todd/Chevalley)
THEOREM: A finite subgroup $G \subset Gl_n(\mathbb{C})$ has
$$\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1, \ldots, f_n] \quad \text{a polynomial ring}$$
$\iff$ G is a complex ref'n group

Chevalley (1955) then gave a classification-free proof of the backward implication.

Springer (1975) nicely separated out the key steps in Chevalley's proof with this:

see notes linked to syllabus

THEOREM: For a finite subgroup $G \subset Gl_n(\mathbb{C})$, T.F.A.E.
(Springer Thm 4.2.5)

(i) G is a complex ref'n group

(ii) $\mathbb{C}[\underline{x}]$ is a free $\mathbb{C}[\underline{x}]^G$-module with finite basis.

(iii) $\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1, \ldots, f_n]$ for alg. indep. homogeneous $f_1, \ldots, f_n$

(i) $\Rightarrow$ (ii) uses some ref'n ideas + some comm. algebra
(ii) $\Rightarrow$ (iii) is all comm. alg.
(iii) $\Rightarrow$ (i) uses Molien's Theorem + generating functions

The ref'n ideas of (i) $\Rightarrow$ (ii) are in the proof of what Humphreys calls...

THE KEY LEMMA:

Assume $f_1 h_1 + \dots + f_m h_m = 0$ for some $f_i \in \mathbb{C}[\underline{x}]^G$, $h_i \in \mathbb{C}[\underline{x}]$

all homogeneous, and $f_1 \notin (f_2, \dots, f_m)_{\mathbb{C}[\underline{x}]^G}$.

Then $h_1 \in I := (\mathbb{C}[\underline{x}]^G_+)_{\mathbb{C}[\underline{x}]}$ = the Hilbert ideal.

---

proof: Induct on $\deg(h_1)$.

BASE CASE: $\deg(h_1) = 0$. WLOG $h_1 = c \in \mathbb{C} - \{0\}$ (else $h_1 \in I$)

so $f_1 = -c^{-1}(f_2 h_2 + \dots + f_m h_m)$

$\Big\downarrow \pi^G$

$f_1 = \pi^G(f_1) = -c^{-1}(f_2 \pi_G(h_2) + \dots + f_m \pi_G(h_m)) \in (f_2, \dots, f_m)_{\mathbb{C}[\underline{x}]^G}$

Contradiction.

INDUCTIVE STEP: $\deg(h_1) \geq 1$.

We make use of the important BGG operators (Bernstein-Gelfand-Gelfand)

for each reflection $s \in G$, with reflecting hyperplane $H = \ker \ell_H(\underline{x})$ for some $\ell_H(\underline{x}) = c_1 x_1 + \dots + c_n x_n$.

CLAIM: Every $h(\underline{x}) \in \mathbb{C}[\underline{x}]$ has $h - s(h)$ vanishing on H,

and hence ℓ_H divides $h - s(h)$ in $\mathbb{C}[\underline{x}]$:

$\forall v \in H$ one has $\big(h - s(h)\big)(v) = h(v) - h(s^{-1}v) = h(v) - h(v) = 0.$

The divisibility is easier to see if one changes basis $x_1, \ldots, x_n$ in V^* so that $\ell_H(\underline{x}) = x_1$

i.e. $H = \{x_1 = 0\}$ and $s = \begin{bmatrix} \zeta & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$

For any $f(\underline{x}) \in \mathbb{C}[\underline{x}]$ vanishing on $H = \{x_1 = 0\}$, then writing $f(\underline{x}) = x_1 \hat{f}(\underline{x}) + \hat{\hat{f}}(x_2, x_3, \ldots, x_n)$ shows $\hat{\hat{f}}(x_2, \ldots, x_n)$ vanishes $\forall\, x_2, \ldots, x_n \in \mathbb{C}^{n-1} \Rightarrow \hat{\hat{f}} = 0.$

The BGG operator for refl'n s is

$$\begin{array}{ccc} \mathbb{C}[\underline{x}] & \xrightarrow{\Delta_s} & \mathbb{C}[\underline{x}] \\ h & \longmapsto & \dfrac{h(\underline{x}) - s(h(\underline{x}))}{\ell_H(\underline{x})} \end{array}$$

and note it $\begin{cases} \text{lowers degree by } 1 \\ \text{is } \mathbb{C}[\underline{x}]^G\text{-linear} \end{cases}$

EXAMPLE $G = \mathfrak{S}_3$ acting on $\mathbb{C}[x_1, x_2, x_3]$

and $s = (1\,2)$ has

$$\Delta_s(x_1^3 x_2^7 x_3^5) = \frac{x_1^3 x_2^7 x_3^5 - s(x_1^3 x_2^7 x_3^5)}{x_1 - x_2} = \frac{x_1^3 x_2^7 x_3^5 - x_1^7 x_2^3 x_3^5}{x_1 - x_2}$$

$$= x_1^3 x_2^3 x_3^5 \frac{(x_2^4 - x_1^4)}{x_1 - x_2} = -x_1^3 x_2^3 x_3^5 (x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3)$$

Now in the inductive step where $\sum_{i=1}^{m} f_i h_i = 0$ with $\deg(h_1) \geq 1$,

apply Δ_s to conclude $\sum_{i=1}^{m} f_i \Delta_s(h_i) = 0$,

and hence $\Delta_s(h_1) \in I = (\mathbb{C}[x]^G_+)_{\mathbb{C}[x]}$ by induction.

$$\Delta_s(h_1) = \frac{h_1 - s(h_1)}{\ell_H}$$

$$\Downarrow$$

$$h_1 - s(h_1) \in \ell_H \cdot I \subset I \quad \forall \text{ refl'ns } s \in G$$

$$\Downarrow$$

$$h_1 = s(h_1) \text{ in } \mathbb{C}[x]/I \quad \forall \text{ refl'ns } s \in G$$

$$\Downarrow$$

$$h_1 = g(h_1) \text{ in } \mathbb{C}[x]/I \quad \forall g \in G$$

$$\Downarrow$$

$$h_1 = \underbrace{\frac{1}{|G|} \sum_{g \in G} g(h_1)}_{= \pi_G(h_1) \in \mathbb{C}[x]^G_+ \subset I} \text{ in } \mathbb{C}[x]/I$$

$$\Downarrow$$

$$h_1 \in I \quad \blacksquare$$

REMARK: Once one has this KEY LEMMA, one can pretty quickly show that any $h_1, \ldots, h_m$ lifting a $\mathbb{C}$-basis for $\mathbb{C}[x]/I$ give a free basis for $\mathbb{C}[x]$ as a free $\mathbb{C}[x]^G$-module; see Springer's Lem 4.2.8

This implication

(ii) $\mathbb{C}[\underline{x}]$ is a free $\mathbb{C}[\underline{x}]^G$-module with finite basis.

$\Downarrow$

(iii) $\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1, \ldots, f_n]$ for alg. indep. homogeneous $f_1, \ldots, f_n$

is a case of a purely comm. alg. statement:

COMM. ALG. LEMMA: (Springer 4.2.10)

Whenever $\mathbb{C}[x_1, \ldots, x_n]$ is a free R-module of finite rank over some $\mathbb{C}$-subalgebra $R \subset \mathbb{C}[\underline{x}]$, then $R = \mathbb{C}[f_1, \ldots, f_n]$ for alg. indep. homog. $f_1, \ldots, f_n$.

The proof is elementary, but rather tricky, and at some point calls on a cute (easy) fact:

EULER'S LEMMA:

If $h(\underline{x}) \in \mathbb{C}[\underline{x}]$ is homog. of degree d,

then $$\sum_{i=1}^{n} x_i \frac{\partial h}{\partial x_i} = d \cdot h(\underline{x})$$

Proof: Check it when $h(\underline{x}) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is a monomial. ▨

REMARK: The map
$$\begin{aligned} \mathbb{C}[\underline{x}] &\longrightarrow \mathbb{C}[\underline{x}] \\ h(\underline{x}) &\longmapsto \left(\sum_{i=1}^{n} x_i \frac{\partial}{\partial x_i}\right) h(\underline{x}) \end{aligned}$$

is sometimes called the Euler derivation.

The implication

(iii) $\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1,\ldots,f_n]$ for alg. indep. homogeneous $f_1,\ldots,f_n$

$\Downarrow$

(i) G is a complex refl'n group

is rather fun, and starts like this...

Assuming $\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1,\ldots,f_n]$ for alg. indep. homog. f_i

name their degrees $d_1 \le d_2 \le \ldots \le d_n$

Let $\hat{G} :=$ the subgroup of G gen'd by all refl'ns in G,

so $\hat{G}$ is a complex refl'n group, and by ((i)$\Rightarrow$(ii)$\Rightarrow$(iii))

already proven, $\mathbb{C}[\underline{x}]^{\hat{G}} = \mathbb{C}[\hat{f}_1,\ldots,\hat{f}_n]$ for alg. indep. homog. $\hat{f}_i$

whose degrees we name $\hat{d}_1 \le \hat{d}_2 \le \ldots \le \hat{d}_n$. GOAL: $G = \hat{G}$.

PROP: In this setting, $\hat{d}_1 \le d_1,\ \hat{d}_2 \le d_2, \ldots, \hat{d}_n \le d_n$.

proof: One has
$$\begin{array}{ccc} \mathbb{C}[\underline{x}]^G & \subset & \mathbb{C}[\underline{x}]^{\hat{G}} \\ \| & & \| \\ \mathbb{C}[f_1,\ldots,f_n] & & \mathbb{C}[\hat{f}_1,\ldots,\hat{f}_n] \end{array}$$

so $\exists$ (unique) polynomials $P_1,\ldots,P_n \in \mathbb{C}[T_1,\ldots,T_n]$

expressing $f_\ell = P_\ell(\hat{f}_1,\ldots,\hat{f}_n)$ for $\ell = 1,2,\ldots,n$,

and whenever the variable T_j appears in $P_\ell(T_1,\ldots,T_n)$

this means $d_\ell \ge \hat{d}_j$.

Note that for each $i = 1, 2, \ldots, n$, one cannot have $\{f_1, f_2, \ldots, f_i\} \subset \mathbb{C}[\hat{f}_1, \hat{f}_2, \ldots, \hat{f}_{i-1}]$

else $\{f_1, f_2, \ldots, f_i\}$ could not be alg. indep.

Hence $\exists$ some f_ℓ with $\ell \leq i$ whose P_ℓ has one of $T_i, T_{i+1}, \ldots, T_n$ appearing, say T_j with $j \geq i$.

This means $$\underbrace{d_i \geq}_{i \geq \ell} \underbrace{d_\ell \geq}_{T_j \text{ appears in } P_\ell} \underbrace{\hat{d}_j \geq}_{j \geq i} \hat{d}_i \qquad \blacksquare$$

We'll then finish it off with an easy consequence of Molien's Theorem (proven below):

(1st numerology PROPOSITION) For a complex refl'n group G, with $\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1, \ldots, f_n]$ homog. of degrees $d_1, \ldots, d_n$ one has

(a) $|G| = d_1 d_2 \cdots d_n$

(b) $\#$ refl'ns in $G = \sum_{i=1}^{n} (d_i - 1)$

EXAMPLE

Recall $\mathbb{C}[\underline{x}]^{G(d,1,n)} = \mathbb{C}[e_1(\underline{x}^d), e_2(\underline{x}^d), \ldots, e_n(\underline{x}^d)]$

degrees: $d \quad 2d \quad \ldots \quad nd$

$\quad\quad\quad\quad\quad\; \| \quad\;\; \| \quad\quad\quad\; \|$

$\quad\quad\quad\quad\quad d_1 \le d_2 \le \ldots \le d_n$

Note $|G(d,1,n)| = \underbrace{d^n}_{\text{choose nonzero entries in } \sqrt[d]{1}} \cdot \underbrace{n!}_{\text{choose the permutation "shape"}} = d \cdot 2d \cdot 3d \cdots nd$ ✓

$\#$refl'ns in $G(d,1,n)$ $= \#\left\{ \begin{bmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \zeta & & \\ & & & & 1 & \\ 0 & & & & & \ddots 1 \end{bmatrix} : \begin{matrix} \zeta \in \sqrt[d]{1} \\ \zeta \neq 1 \end{matrix} \right\} + \#\left\{ \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & & \zeta^{-1} & \\ & & & \ddots & & \\ & & \zeta & & 0 & \\ & & & & & \ddots 1 \end{bmatrix} : \zeta \in \sqrt[d]{1} \right\}$

$= (d-1) \cdot n + \binom{n}{2} d = \binom{n+1}{2} d - n$

$= (d-1) + (2d-1) + \ldots + (nd-1)$ ✓

Why does this finish off (iii) $\Rightarrow$ (i) ?

Recall we want to show the inclusion $\hat{G} \le G$ is equality.

Note $G, \hat{G}$ have the same set of refl'ns,

so part (b) and $\hat{d}_i \le d_i \Rightarrow \hat{d}_i = d_i \; \forall i$.

Then part (a) $\Rightarrow |\hat{G}| = |G|$,

so $G = \hat{G}$, a refl'n group ▨

Molien's THEOREM (1897) - invariant theory numerology workhorse!

It says that for G a finite subgroup of $GL_n(\mathbb{C})$ acting on $\mathbb{C}[\underline{x}] = \mathbb{C}[x_1, \ldots, x_n]$ as before, the invariant ring $\mathbb{C}[\underline{x}]^G$ has Hilbert series

$$\mathrm{Hilb}(\mathbb{C}[\underline{x}]^G, q) \overset{\text{DEF'N}}{:=} \sum_{d=0}^{\infty} q^d \dim_{\mathbb{C}}\left(\mathbb{C}[\underline{x}]^G_d\right)$$

computable by another average over G:

$$\mathrm{Hilb}(\mathbb{C}[\underline{x}]^G, q) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - q \cdot g)}$$

EXAMPLE: $G = \mathfrak{S}_2$ acting on $\mathbb{C}[x_1, x_2]$ has $\mathbb{C}[x_1, x_2]^{\mathfrak{S}_2} = \mathbb{C}[\overset{\text{degrees } 1}{e_1}, \overset{2}{e_2}]$

$$\Rightarrow \mathrm{Hilb}(\mathbb{C}[\underline{x}]^{\mathfrak{S}_2}, q) = (1 + q^1 + q^2 + \cdots)(1 + q^2 + (q^2)^2 + \cdots) = \frac{1}{(1-q^1)(1-q^2)}$$

while Molien says

$$\mathrm{Hilb}(\mathbb{C}[\underline{x}]^{\mathfrak{S}_2}, q) = \frac{1}{2!}\left[\frac{1}{\det\left(I_2 - q\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)} + \frac{1}{\det\left(I_2 - q\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)}\right]$$

$$= \frac{1}{2}\left[\frac{1}{\det\begin{bmatrix} 1-q & 0 \\ 0 & 1-q \end{bmatrix}} + \frac{1}{\det\begin{bmatrix} 1 & -q \\ -q & 1 \end{bmatrix}}\right] = \frac{1}{2}\left[\frac{1}{(1-q)^2} + \frac{1}{(1-q^2)}\right]$$

$$= \frac{1}{2(1-q)(1-q^2)}\left[(1+q) + (1-q)\right] = \frac{1}{(1-q)(1-q^2)} \checkmark$$

proof of Molien's Thm:

Let's interpret each term $\dfrac{1}{\det(I_n - q\cdot g)}$ as a graded trace.

Change the $\mathbb{C}$-basis $x_1,\dots,x_n$ for V^* so g acts triangularly with eigenvalues $\lambda_1,\dots,\lambda_n$:

$$g = \begin{array}{c} \\ x_1 \\ \vdots \\ x_n \end{array}\begin{array}{c} \begin{array}{ccc} x_1 & \cdots & x_n \end{array} \\ \begin{bmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} \end{array} \qquad \left(\text{i.e. } g^{-1} = \begin{array}{c} \\ e_1 \\ \vdots \\ e_n \end{array}\begin{array}{c} \begin{array}{ccc} e_1 & \cdots & e_n \end{array} \\ \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ * & & \lambda_n \end{bmatrix} \end{array} \text{ on } V\right)$$

Then g also acts triangularly on the $\mathbb{C}$-basis $\{x_1^{a_1}\cdots x_n^{a_n}\}_{a_1+\dots+a_n=d}$ for $\mathbb{C}[\underline{x}]_d$

with eigenvalues $\{\lambda_1^{a_1}\cdots\lambda_n^{a_n}\}_{a_1+\dots+a_n=d}$,

if we order the monomials lexicographically:

e.g. $n=2$, $d=3$

$$g = \begin{array}{c} \\ x_1 \\ x_2 \end{array}\begin{array}{c} \begin{array}{cc} x_1 & x_2 \end{array} \\ \begin{bmatrix} \lambda_1 & c \\ 0 & \lambda_2 \end{bmatrix} \end{array} \Rightarrow \begin{array}{c} \\ x_1^3 \\ x_1^2x_2 \\ x_1x_2^2 \\ x_2^3 \end{array}\begin{array}{c} \begin{array}{cccc} x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \begin{bmatrix} \lambda_1^3 & & & \\ & \lambda_1^2\lambda_2 & * & \\ & 0 & \lambda_1\lambda_2^2 & \\ & & & \lambda_2^3 \end{bmatrix} \end{array}$$

Hence $\displaystyle\sum_{d=0}^{\infty} q^d \cdot \mathrm{Trace}\left(\mathbb{C}[\underline{x}]_d \xrightarrow{g} \mathbb{C}[\underline{x}]_d\right)$ ← graded trace of g on $\mathbb{C}[\underline{x}]$

$$= \sum_{d=0}^{\infty} q^d \cdot \sum_{a_1+\dots+a_n=d} \lambda_1^{a_1}\cdots\lambda_n^{a_n} = (1+\lambda_1 q+\lambda_1^2q^2+\dots)\cdots(1+\lambda_n q+\lambda_n^2q^2+\dots)$$

$$= \frac{1}{(1-\lambda_1 q)\cdots(1-\lambda_n q)} = \frac{1}{\det\begin{bmatrix} 1-\lambda_1 q & & 0 \\ & \ddots & \\ * & & 1-\lambda_n q \end{bmatrix}} = \frac{1}{\det(I_n - q\cdot g^{-1})}$$

Now recall…

EXERCISE: For any fin. dim'l G-rep'n U one has $\dim_{\mathbb{C}}(U^G) = \mathrm{Trace}\left(U \xrightarrow{\pi_G} U\right)$,

because $\pi_G^2 = \pi_G$ shows $U = \underset{\text{1-eigenspace}}{\mathrm{im}(\pi_G)} \oplus \underset{\text{0-eigenspace}}{\ker(\pi_G)}$

i.e.
$$\pi_G = \begin{array}{c|c} & \begin{array}{cc} U^G & \ker(\pi_G) \end{array} \\ \hline \begin{array}{c} U^G \\ \\ \ker(\pi_G) \end{array} & \left[\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right] \end{array}$$

Hence
$$\mathrm{Hilb}(\mathbb{C}[x]^G, q) = \sum_{d=0}^{\infty} q^d \cdot \dim_{\mathbb{C}} \left(\mathbb{C}[x]_d\right)^G$$
$$= \sum_{d=0}^{\infty} q^d \cdot \mathrm{Trace}\left(\mathbb{C}[x]_d \xrightarrow{\pi_G} \mathbb{C}[x]_d\right)$$

$\mathrm{Trace}(\pi_G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Trace}(g)$

$$= \frac{1}{|G|} \sum_{g \in G} \sum_{d=0}^{\infty} q^d \cdot \mathrm{Trace}\left(\mathbb{C}[x]_d \xrightarrow{g} \mathbb{C}[x]_d\right)$$
$$= \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - q \cdot g^{-1})}$$
$$= \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - q \cdot g)} \qquad \blacksquare$$

Now let's use it to prove ...

(1st numerology PROPOSITION) For a complex refl'n group G, with $\mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1, \ldots, f_n]$ homog. of degrees $d_1, \ldots, d_n$ one has (a) $|G| = d_1 d_2 \cdots d_n$

(b) $\#$ refl'ns in $G = \sum_{i=1}^{n} (d_i - 1)$

proof: Compare 2 expressions for $\mathrm{Hilb}(\mathbb{C}[\underline{x}]^G, q)$:

$$\underbrace{\frac{1}{|G|}\sum_{g \in G} \frac{1}{\det(I_n - q \cdot g)}}_{\text{from Molien}} = \underbrace{\frac{1}{(1-q^{d_1}) \cdots (1-q^{d_n})}}_{\text{from } \mathbb{C}[\underline{x}]^G = \mathbb{C}[f_1, \ldots, f_n]}$$

$$\frac{1}{|G|}\sum_{g \in G} \frac{1}{(1-q\lambda_1(g)) \cdots (1-q\lambda_n(g))}$$

if g has eigenvalues $\lambda_1(g), \ldots, \lambda_n(g)$

$$= \frac{1}{|G|}\left(\frac{1}{(1-q)^n} + \sum_{\substack{\text{refl'ns} \\ s \in G}} \frac{1}{(1-q)^{n-1}(1-q \cdot \det(s))} + \frac{f(q)}{(1-q)^{n-2}} \right)$$

where $f(q)$ has no pole at $q=1$.

mult. both sides by $(1-q)^n$

$$\frac{1}{|G|}\left(1+\sum_{\substack{\text{refl'ns}\\ s\in G}}\frac{1-q}{1-q\cdot\det(s)}+(1-q)^2 f(q)\right)\overset{(*)}{=}\prod_{i=1}^{n}\frac{1-q}{1-q^{d_i}}=\frac{1}{[d_1]_q\cdots[d_n]_q}$$

where
$$[d]_q = 1+q+q^2+\dots+q^{d-1}$$

$\lim_{q\to 1}$

$$\frac{1}{|G|}\left(1+\sum_{\substack{\text{refl'ns}\\ s\in G}}0+0\right)=\frac{1}{d_1 d_2\cdots d_n}$$

$$\Longrightarrow \quad |G| = d_1 d_2\cdots d_n$$

take $\frac{d}{dq}$

$\hat{f}(q)$ also has no pole at $q=1$

$$\frac{1}{|G|}\left(0+\sum_{\substack{\text{refl'ns}\\ s\in G}}\frac{(1-q\det(s))(-1)+(1-q)\det(s)}{(1-q\cdot\det(s))^2}+(1-q)\hat{f}(q)\right)$$

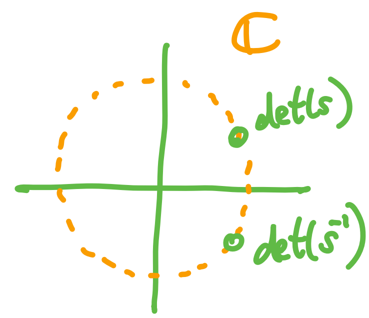
$$=-\prod_{i=1}^{n}\frac{1}{[d_i]_q}\sum_{i=1}^{n}\frac{1+2q+3q^2+\dots+(d-1)q^{d-2}}{[d_i]_q}$$

$\lim_{q\to 1}$

$$\frac{1}{|G|}\sum_{\substack{\text{refl'ns}\\ s\in G}}\frac{-1}{1-\det(s)} = \frac{-1}{d_1 d_2\cdots d_n}\sum_{i=1}^{n}\frac{\binom{d_i}{2}}{d_i}$$

Since $|G| = d_1 d_2 \cdots d_n$, this means

$$\sum_{\substack{\text{refns} \\ s \in G}} \frac{1}{1-\det(s)} = \sum_{i=1}^{n} \frac{d_i - 1}{2}$$



$$\| $$

$$\frac{1}{2} \sum_{\substack{\text{ref'ns} \\ s \in G}} \underbrace{\left(\frac{1}{1-\det(s)} + \frac{1}{1-\det(s^{-1})} \right)}_{= \frac{1-\det(s^{-1}) + 1-\det(s)}{(1-\det(s))(1-\det(s^{-1}))} = \frac{2-(\det(s)+\det(s^{-1}))}{1-(\det(s)+\det(s^{-1}))+1} = 1 \; (!)}$$

$$\|$$

$$\frac{\#\text{ref'ns in } G}{2}$$

$$\Longrightarrow \#\text{refns in } G = \sum_{i=1}^{n} (d_i - 1) \qquad \blacksquare$$

REMARK:

The (iii) $\Rightarrow$ (i) proof via Molien & generating functions was all in the Shephard & Todd 1955 paper.