Rings of invariants of finite groups

- Hilbert + Noether results for invariant rings of finite subgroups of GL in the non-modular case.
- Molien's formula for the Hilbert series of the ring of invariants, Some examples.
- Cohen-Macaulay property of the ring of invariants.

Symmetric polynomials: k -- a field, $\mathrm{char}(k)=0$, $x=(x_1,\dots,x_n)$
$k[x]=k[x_1,\dots,x_n]$, $S_n \equiv$ symmetric group on $[n]=\{1,2,\dots,n\}$

Def 1: $f(x_1,\dots,x_n)\in k[x]$ is called symmetric pol. if $\forall\, \sigma\in S_n$
$$f(x_1,\dots,x_n)=f(x_{\sigma(1)},x_{\sigma(2)},\dots,x_{\sigma(n)}).$$
They form a subring of $k[x]$, notation is $k[x]^{S_n}$.

The coefficients of $g\equiv g(t)=(t-x_1)\dots(t-x_n)=t^n-e_1t^{n-1}+\dots+(-1)^ne_n$
with $e_1=x_1+x_2+\dots+x_n$, $e_2=\sum_{1\le i<j\le n} x_ix_j$, $\dots$, $e_n=x_1\cdot x_2\cdot\ldots\cdot x_n$.

Def 2: $e_i\equiv e_i(x_1,\dots,x_n)$, $i=1,\dots,n$, are (called) the ~~sy~~ elementary symmetric pol. in $x_1,\dots,x_n$.

Th 3: (Fund. th. on symm. pol.) $\forall$ sym. pol. is uniquely written as a polyn. in $e_1,\dots,e_n$.

Pf: (existence) There is total order of monomials in $k[x]$ given by dlo $\equiv$ degree lexicographic order: $\alpha=(\alpha_1,\dots,\alpha_n)$
$\beta=(\beta_1,\dots,\beta_n)\in\mathbb{N}^n$, $\mathbb{N}=\{0,1,2,\dots\}$

$x^\alpha=x_1^{\alpha_1}\dots x_n^{\alpha_n}$
$|\alpha|=\alpha_1+\alpha_2+\dots+\alpha_n$

$x^\alpha<x^\beta$ iff
- either $|\alpha|<|\beta|$
- or $|\alpha|=|\beta|$ and $\exists\, r$ s.t. $\alpha_1=\beta_1,\dots,\alpha_{r-1}=\beta_{r-1}$ and $\alpha_r<\beta_r$

Algorithm ("induction degree" based on dlo): $f\in k[x]$ given by lin. comb. of monomials the largest mon. for dlo applied to f is $\mathrm{dlo}(f)$. If x^α occurs in f, then $\sigma(x^\alpha) = x^{\sigma(\alpha)}$ also occurs in f, hence $\mathrm{dlo}(f) = c\, x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, $c \in k^*$ and $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$; here $\sigma(\alpha) = \sigma(\alpha_1, \alpha_2, \dots, \alpha_n) = (\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \dots, \alpha_{\sigma(n)})$. We have

$$\mathrm{dlo}\left(e_1^{\beta_1} e_2^{\beta_2} \cdots e_n^{\beta_n}\right) = \prod_{i=1}^{n} x_i^{\beta_i + \beta_{i+1} + \dots + \beta_n}, \text{ so}$$

$$\mathrm{dlo}\left(e_1^{\alpha_1 - \alpha_2} e_2^{\alpha_2 - \alpha_3} \cdots e_n^{\alpha_{n-1} - \alpha_n} e_n^{\alpha_n}\right) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

for all $(\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. Therefore, $\tilde{f} := f - c\, e_1^{\alpha_1 - \alpha_2} \cdots e_n^{\alpha_{n-1} - \alpha_n} e_n^{\alpha_n}$ fulfills $\mathrm{dlo}(\tilde{f}) < \mathrm{dlo}(f)$. As there are finitely many monomials $\leq$ a given monomial w.r.t. dlo, the algorithm teminates after finitely many steps.

(Uniqueness:) follow from the fact that $e_1, e_2, \dots, e_n$ are algebr. independent (left as an exercise). ▨

Some other basis/generators of symmetric polynomials (ring):

Power sum symm. pol.

Def 4: The polynomials $p_k = p_k(x_1, \dots, x_n) = x_1^k + \dots + x_n^k$, $k \in \mathbb{N}$, are (called) power sum symm. polyn.

Th 5: (Newton's identities)

$$p_k \equiv p_k(x_1, \dots, x_n) = \begin{cases} e_1 p_{k-1} - e_2 p_{k-2} + \dots + (-1)^{n-1} e_n p_{k-n} & \text{for } k > n \\ e_1 p_{k-1} - e_2 p_{k-2} + \dots + (-1)^{k-2} p_1 e_{k-1} + (-1)^{k-1} k e_k & \text{for } k \leq n \end{cases}$$

Pf: $E \equiv E(t) = (1 - t x_1)(1 - t x_2) \cdots (1 - t x_n) = 1 - e_1 t + e_2 t^2 - \dots + (-1)^n e_n t^n$, then $\frac{d}{dt}$-derivative of $\log E(t) = \sum_{i=1}^{n} \log(1 - t x_i)$ gives

$$-\frac{E'(t)}{E(t)} = \sum_{i=1}^{n} \frac{x_i}{1 - t x_i} = \sum_{i=1}^{n} x_i \sum_{k=0}^{\infty} (t x_i)^k = \sum_{k=0}^{\infty} \sum_{i=1}^{n} x_i^{k+1} t^k = \sum_{k=1}^{\infty} p_k t^{k-1}$$

$$\Rightarrow \quad E'(t) = -E(t) \sum_{k=1}^{\infty} p_k t^{k-1},$$ and the substitution for $E(t)$

gives in each graded component t^j the required relation. ■

Corollary 6 For $k \leq n$,

$$p_k = \begin{vmatrix} e_1 & 1 & 0 & \cdots & 0 \\ 2e_2 & e_1 & 1 & & \vdots \\ 3e_3 & e_2 & e_1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ ke_k & e_{k-1} & e_{k-2} & \cdots & e_1 \end{vmatrix}, \qquad k!\, e_k = \begin{vmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & & \vdots \\ \vdots & \vdots & p_1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & & k-1 \\ p_k & p_{k-1} & p_{k-2} & \cdots & p_1 \end{vmatrix}$$

Pf: Newton's identities

$$\left.\begin{aligned} p_1 &= e_1 \\ p_2 &= e_1 p_1 - 2e_2 \\ p_3 &= e_1 p_2 - e_2 p_1 + 3e_3 \\ &\vdots \end{aligned}\right\} \Rightarrow \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ p_1 & -2 & 0 & & \vdots \\ p_2 & -p_1 & 3 & & \vdots \\ \vdots & \vdots & p_1 & & \\ p_{k-1} & -p_{k-2} & \vdots & & (-1)^k k \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix}$$

and by Cramer's rule + column exchange $\Rightarrow$ formula for $k!\,e_k$.

$$\left.\begin{aligned} e_1 &= p_1 \\ 2e_2 &= p_1 e_1 - p_2 \\ 3e_3 &= p_1 e_2 - p_2 e_1 + p_3 \\ &\vdots \\ ke_k &= p_1 e_{k-1} - p_2 e_{k-2} + \dots + (-1)^{k-1} p_k \end{aligned}\right\} \Rightarrow \begin{bmatrix} 1 & 0 & & & 0 \\ e_1 & -1 & & & \vdots \\ e_2 & -e_1 & 1 & & \vdots \\ \vdots & \vdots & & -1 \ddots & \vdots \\ & & & & 0 \\ e_{k-1} & -e_{k-2} & & & (-1)^{k-1} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix} = \begin{bmatrix} e_1 \\ 2e_2 \\ \vdots \\ ke_k \end{bmatrix}.$$

This solves for p_k with required formulas. ■

Complete homogeneous polynomials

Def 7: The complete homogeneous polyn. h_r, $r \in \{1,2,3,\dots\}$, are defined by
$$h_r \equiv h_r(x_1,\dots,x_n) = \sum_{\substack{\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n \\ |\alpha| = r}} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$
We define $h_0 = 1$ and $h_r = 0$ for $r < 0$.

Corollary 8: For $r \in \{1,2,3,\dots,n\}$, we have

$$e_r = \begin{vmatrix} h_1 & 1 & 0 & \cdots & 0 \\ h_2 & h_1 & 1 & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \cdots & 1 \\ h_r & h_{r-1} & h_{r-2} & & h_1 \end{vmatrix}, \qquad h_r = \begin{vmatrix} e_1 & 1 & 0 & \cdots & 0 \\ e_2 & e_1 & 1 & & \vdots \\ \vdots & \vdots & e_1 & & \vdots \\ \vdots & \vdots & \vdots & & 1 \\ e_r & e_{r-1} & e_{r-2} & & e_1 \end{vmatrix}$$

Pf: The generating function for $\{h_r\}_r$ fulfills

$$H \equiv H(t) = \sum_{r=0}^{\infty} h_r t^r = \prod_{i=1}^{n} (1 + x_i t + x_i^2 t^2 + \ldots) = \prod_{i=1}^{n} (1 - x_i t)^{-1} = E^{-1}(t)$$

$\Rightarrow H(t)E(t) = 1$, and the coefficient by t^i, $i \in \{1, 2, \ldots, r\}$, gives

$-h_1 = -e_1$, $-h_2 = -e_1 h_1 + e_2$, $-h_3 = -e_1 h_2 + e_2 h_1 - e_3$, ...,

$-h_r = -e_1 h_{r-1} + e_2 h_{r-2} - \ldots + (-1)^r e_r$

and solve again by Cramer's rule for e_r, h_r. ∎

Corollary 9: For $r \in \{1, 2, \ldots, n\}$, we have

$$r!\, h_r = \begin{vmatrix} p_1 & -1 & 0 & 0 & \cdots & 0 \\ p_2 & p_1 & -2 & 0 & & \vdots \\ p_3 & p_2 & p_1 & -3 & & \vdots \\ \vdots & \vdots & \vdots & p_1 & & 0 \\ p_{r-1} & p_{r-2} & \vdots & \vdots & \cdots & -(r-1) \\ p_r & p_{r-1} & & & & p_1 \end{vmatrix}$$

Pf: $\frac{d}{dt}\log$ applied to $H(t) = \sum_{r=0}^{\infty} h_r t^r = \prod_{i=1}^{n} (1 - x_i t)^{-1}$, we get

$$H'(t) = H(t) \sum_{r=1}^{\infty} p_r t^{r-1} \quad \left(\text{recall } H \cdot E = 1,\ -\frac{d}{dt} \log E = \sum_{k=1}^{\infty} p_k t^{k-1} \right)$$

$$\Rightarrow \left. \begin{array}{l} p_1 = h_1 \\ p_2 = -p_1 h_1 + 2h_2 \\ \vdots \\ p_r = -p_{r-1} h_1 - p_{r-2} h_2 - \ldots + r h_r \end{array} \right\} \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ p_1 & -2 & 0 & & \vdots \\ p_2 & p_1 & -3 & & \vdots \\ \vdots & \vdots & \vdots & & 0 \\ p_{r-1} & p_{r-2} & p_{r-3} & & -r \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_r \end{bmatrix} = \begin{bmatrix} -p_1 \\ -p_2 \\ \vdots \\ -p_r \end{bmatrix}$$

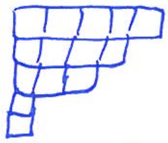
and the claim follows by Cramer's rule again. ∎

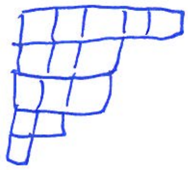
Schur polynomials

Partition = a finite sequence $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\lambda_i \in \mathbb{N}$, in decreasing order $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$, two partitions which differ by terminal zeroes are regarded as equivalent

(Non-zero) λ_i are parts of λ, $\#\lambda_i = n \equiv \ell(\lambda)$ is the length of λ

The sum $|\lambda| := \sum_{i=1}^{n} \lambda_i$ is the weight of λ.

If $|\lambda| = k$, $\lambda \equiv$ partition of k is represented by Young diagram: $\lambda = (5,4,3,1,1) \leftrightarrow$ , the conjugate λ' of λ has its Young diagram the transpose of λ: for $\lambda = (5,4,3,1,1)$ is $\lambda' = (5,3,3,2,1) \longleftrightarrow$



For $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, $\underset{\sigma \in S_n}{\sigma(x^\alpha)} = x_{\sigma(1)}^{\alpha_1} x_{\sigma(2)}^{\alpha_2} \cdots x_{\sigma(n)}^{\alpha_n}$

define the polynomial $a_\alpha(x_1, \dots, x_n) := \sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\, \sigma(x^\alpha) \equiv a_\alpha$.

We have $\sigma'(a_\alpha) = \operatorname{sign}(\sigma')\, a_\alpha \ \forall \sigma' \in S_n \Rightarrow a_\alpha$ is skew-symmetric $\Rightarrow a_\alpha = 0$ unless $\forall\ \alpha_1, \alpha_2, \dots, \alpha_n$ are distinct, so we may assume $\alpha_1 > \alpha_2 > \dots > \alpha_n \geq 0$. Write $\alpha = (\lambda_1, \lambda_2, \dots, \lambda_n) + \underbrace{(n-1, n-2, \dots, 2, 1, 0)}_{\delta}$, then $\lambda = (\lambda_1, \dots, \lambda_n)$ is a partition. We compute

$a_\alpha = \det(A)$, $A = \{a_{ij}\}_{i,j=1}^n$ with $a_{ij} = x_i^{\alpha_j}$, and in particular

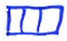
$a_\delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ (Vandermonde determinant). Since

$a_\delta \mid a_{\lambda+\delta}$ ($\Leftarrow \forall$ roots of a_δ are roots of $a_{\lambda+\delta}$), ~~and so~~ $S_\lambda := \dfrac{a_{\lambda+\delta}}{a_\delta}$ is a symmetric polynomial.

Def 10: The symmetric polyn. $S_\lambda = S_\lambda(x_1, \dots, x_n)$ is the Schur polyn. corresponding to the partition λ.

Rem 11: $\deg(S_\lambda) = |\lambda|$.

Example 12: $\lambda = (1,1,1) \leftrightarrow$ , $\delta = (2,1,0)$, $\dfrac{a_{\lambda+\delta}}{a_\delta} = \dfrac{\begin{vmatrix} x_1^3 & x_1^2 & x_1 \\ x_2^3 & x_2^2 & x_2 \\ x_3^3 & x_3^2 & x_3 \end{vmatrix}}{a_\delta} = x_1 x_2 x_3 = \underset{\text{elem. sym. pol.}}{\underset{\shortparallel}{e_3}}$

Example 13: $\lambda = (3,0,0) \leftrightarrow$ , $\delta = (2,1,0)$, $\dfrac{a_{\lambda+\delta}}{a_\delta} = \dfrac{\begin{vmatrix} x_1^5 & x_1 & 1 \\ x_2^5 & x_2 & 1 \\ x_3^5 & x_3 & 1 \end{vmatrix}}{a_\delta} = h_3$ = complete homog. polyn.

Prop. 14: The set $\{ S_\lambda \mid \lambda = (\lambda_1, .., \lambda_n)$ partition, $|\lambda| = d \}$ is a basis of the vector space of all sym. pol. of degree d in $x_1, .., x_n$.

Pf: P_A .. vector space of skew-symmetric polynomials ($p \in P_A$ if $\sigma \cdot p = \mathrm{sgn}(\sigma) p \ \forall \sigma \in S_n$), $a_\delta \in P_A$ pol. given by Vandermonde determinant. If $f \in P_A$, then $f = g a_\delta$ for $g \in k[x]^{S_n}$. Define the linear map

$$\mu : k[x]^{S_n} \longrightarrow P_A$$
$$g \longmapsto \mu(g) := g \cdot a_\delta .$$

μ is a vector space isomorphism and Schur polyn. map to all skew-symmetric monomials. Since such monomials constitute a basis of P_A, the Schur polyn. are basis of $k[x]^{S_n}$. ▨

Prop. 15: A_n = alternating group ($= \mathrm{Ker}(\mathrm{sgn} : S_n \to \mathbb{Z}_2)$, i.e. normal subgroup of S_n.) Then $\forall f \in k[x]^{A_n}$ is uniquely written as $f = g + h a_\delta$, $g, h \in k[x]^{S_n}$ (symmetr. pol.)

Pf: For $\sigma \in S_n$, $(\sigma \cdot f)(x_1, .., x_n) = f(x_{\sigma(1)}, .., x_{\sigma(n)})$, define $\tau := (12)$
the action of S_n on f $\quad$ $\mathrm{sgn}(\tau) = -1$.

Set $g := \frac{1}{2}(f + \tau f)$, $\tilde{g} := \frac{1}{2}(f - \tau f)$. Then g is symmetric and $\tilde{g}$ is skew-symmetric polynomial, therefore $a_\delta \mid \tilde{g}$. Writing $\tilde{g} = a_\delta h$, $h \in k[x]^{S_n}$ symmetric polyn., $f = g + a_\delta h$. Assuming $g_1, h_1 \in k[x]^{S_n}$ symm. pol. such that $f = g_1 + a_\delta h_1$, we get $g - g_1 = a_\delta (h_1 - h)$, and since the only polynomial which is both symmetric and skew-symmetric is the trivial one, $g = g_1$ and $h = h_1$, hence uniqueness follows. ▨

Hilbert and Noether theorems

$k[x] = k[x_1, .., x_n]$, $G < GL(n, k)$ finite subgrp

$k[x]^G := \{ f \in k[x] \mid g \cdot f = f \ \forall g \in G \}$, $g \in GL(n,k)$ acts by $(x_1, .., x_n)^T \longmapsto g \cdot (x_1, .., x_n)^T$ extends to $k[x]$ so that $f \mapsto g \cdot f$

is an automorphism of $k[x]$. Basic problems of invariant theory for G are:

a/ Find the set of generators of $k[x]^G$ (= fundamental invariants)

b/ Relations among the fundamental invariants (syzygies)

c/ Represent an arbitrary invariant in terms (as a polynomial) of fundamental invariants

d/ Relate geometric properties of G, k^n/G, with invariants $k[x]^G$.

E.g., $k[x]^{S_n}$ is generated by n-tuple of symm. pol. (element. symm. fcions), are alg. independent $\Rightarrow$ $k[x]^{S_n}$ has transc. degree n over k. The same holds in greater generality:

<u>Prop 16</u>: The ring $k[x]^G$ has transc. degree n over k.

<u>Pf</u>: tr deg = transcendence degree; $\mathrm{trdeg}_k\, k[x] = n$. Thus it is enough to show that $x_1, \dots, x_n$ are algebraic over $k[x]^G$.

Define, for $i = 1, 2, \dots, n$: $P_i(t) := \prod_{g \in G} (t - g\cdot(x_i))$,

and observe:

- the coefficients of $P_i(t)$ are in $k[x]^G$
- $P_i(x_i) = 0$

$\Big\} \Rightarrow$ x_i is integral over $k[x]^G$ $\forall i \in \{1, 2, \dots, n\}$

$\Rightarrow$ $k[x]$ and $k[x]^G$ have the same trdeg_k. ▨

For $(R, +, \cdot, 1)$ comm. unit ring, $f: R \to R$ a ring automorphism if it is a bijective ring homomorphism $R \to R$. The set of $\forall$ automorphisms of R, $\mathrm{Aut}(R)$, forms a group. Let R, $G < \mathrm{Aut}(R)$, $|G|$ invertible in R. Consider the map $\rho: R \to S := R^G$ ← the ring of G-invariants in R,

defined as $\rho: r \to \rho(r) := \frac{1}{|G|} \sum_{g \in G} g\cdot r$. Then

- ρ is S-linear
- $\rho|_S = \mathrm{Id}_S$

$\Big\}$ $\rho: R \to S = R^G$ is Reynolds operator for (R, S), $S \subseteq R$

Prop. 17: Let $S \subseteq R$ a subring, $\rho : R \to S$ Reynolds operator. Then

a/ $IR \cap S = I$ $\forall$ $I \subset S$ ideals in S,

b/ If R is Noetherian, then so is S.

Pf: "$\supset$" is trivial; "$\subset$" follows from taking $\sum a_i r_i = a \in S$ with

a) $a_1, \dots, a_n \in I$, $r_1, \dots, r_n \in R$, so that $a = \rho(a) = \sum_i \rho(r_i) a_i \in I$.

b/ $I_1 \subseteq I_2 \subseteq \dots$ ascending chain of ideals in R, then $I_n R = I_{n+1} R = \dots$ for some $n \in \mathbb{N}$, since R is Noetherian. By a/, $I_n = I_n R \cap S = I_{n+1} R \cap S = I_{n+1} = I_{n+2} = \dots$, and S is Noetherian. ▨

Theorem 18 (Hilbert finiteness theorem) $G \leq GL(n, k)$ a subgroup acting linearly on $k[x] = R$ (not necessarily finite.) Assume there is a Reynolds operator $\rho : R \to S$, $S = k[x]^G$. Then S is a finitely generated k-algebra.

Pf: $I_S \equiv$ the maximal ideal of S, generated by homog. elements of positive degree; since R is Noetherian, $I_S R$ has finitely many generators and we denote them $f_1, f_2, \dots, f_s \in I_S$.

We shall prove that $S = k[x]^G = k[f_1, f_2, \dots, f_s]$. Assume $f \in S$ is homogeneous of degree d, and apply induction on d. If $d = 0$, $f \in k$, so suppose $d > 0$, hence $f \in I_S$. By Prop 17, a/, $\exists\, g_1, \dots, g_s \in R$ s.t. $f = g_1 f_1 + \dots + g_s f_s$. The application of ρ to both sides gives $f = \rho(g_1) f_1 + \dots + \rho(g_s) f_s$. Because $G < GL(n, k)$, G preserves grading on $k[x]$ and so we (may) assume $f, f_1, \dots, f_s, g_1, \dots, g_s$ are homogeneous. Then $\deg(g_i) = \deg(f) - \deg(f_i) < \deg(f)$ (recall $\deg(f_i) > 0$ for all $i = 1, \dots, s$) $\Rightarrow$ by induction on degree we assume $\rho(g_1), \dots, \rho(g_s) \in k[f_1, f_2, \dots, f_s]$ $\Rightarrow f \in k[f_1, f_2, \dots, f_s]$. ▨

$\deg(g_i) = \deg \rho(g_i)$

Corollary 19: $G < GL(n, k)$ finite group, acting linearly on $k[x]$, and assume $(|G|, \mathrm{char}\, k) = 1$. Then $k[x]^G$ is finitely generated k-algebra.

Th 20: (Noethers bound) $G < GL(n,k)$ a finite subgroup of order $|G|$ s.t. $(|G|, \mathrm{char}\, k) = 1$. Then $k[x]^G$ is generated by at most $\binom{n+|G|}{n}$ invariants of degree at most $|G|$.

Pf: $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $\rho(x^\alpha) = \frac{1}{|G|} \sum_{\tilde{g} \in G} \tilde{g}(x^\alpha)$, $\tilde{g} \in G < \mathrm{Aut}(k[x])$.

For $f(x) = \sum_\alpha f_\alpha x^\alpha$, $f_\alpha \in k$, a G-invariant, $\tilde{g}(x^\alpha) = \tilde{g}(x_1^{\alpha_1}) \dots \tilde{g}(x_n^{\alpha_n})$, so that $f = (\rho f)(x_1, \dots, x_n) = \frac{1}{|G|} \sum_{\alpha, \tilde{g} \in G} \tilde{g}(x_1)^{\alpha_1} \dots \tilde{g}(x_n)^{\alpha_n} \Rightarrow$

f is a lin. combination of invariants $\sum_{\tilde{g} \in G} \tilde{g}(x^\alpha) =: J_\alpha$.

For $\overbrace{u_1, \dots, u_n}^{u}$ variables, in the polynomial

$S_d(u) = \sum_{\tilde{g} \in G} (u_1 \tilde{g}(x_1) + \dots + u_n \tilde{g}(x_n))^d$, $d = |\alpha|$, J_α is the coefficient of $u_1^{\alpha_1} \dots u_n^{\alpha_n}$ (up to a k-multiple). Notice that $S_d(u)$ is d-th power sum in $|G|$ polynomials $u_1 \tilde{g}(x_1) + \dots + u_n \tilde{g}(x_n)$. By Newton's identities, $S_d(u)$ ~~are~~ polynomials in the first $|G|$-tuple of them, $\underbrace{S_1(u), S_2(u), \dots, S_{|G|}(u)}_{|G|-\text{tuple}}$. This implies $\forall$ G-invariants J_α, $|\alpha| > |G|$, are in the subring $k[J_\alpha \mid |\alpha| \leq |G|] \Rightarrow k[x]^G$ is generated by $\binom{n+|G|}{n}$ invariants $\rho(x^\alpha)$, $|\alpha| \leq |G|$. ∎

Lemma 21 (Noethers bound is optimal) $p \in \mathbb{N}$ prime, $\mathbb{N} \ni n \geq 2$, $k = \mathbb{C}$. Let $G = \{\mathrm{diag}(\xi_p^k, \xi_p^k, \dots, \xi_p^k) \mid k \in \{0, 1, \dots, p-1\}\}$, $\xi_p := e^{2\pi i/p}$ p-th (primitive) root of 1, be the cyclic group of order $p = |G|$. Then $\mathbb{C}[x]^G = \mathbb{C}[x^\alpha \mid |\alpha| = p]$.

Pf: $\rho: \mathbb{C}[x] \to \mathbb{C}[x]^G$ the Reynolds operator. Then

$$\rho(x^\alpha) = \frac{1}{p} \sum_{k=0}^{p-1} (\xi_p^k x_1)^{\alpha_1} \dots (\xi_p^k x_n)^{\alpha_n} = \frac{1}{p} \sum_{k=0}^{p-1} \xi_p^{k|\alpha|} x^\alpha$$

$$= \frac{x^\alpha}{p} \sum_{k=0}^{p-1} \xi_p^{k|\alpha|},$$

and if $(\overset{|G|}{\overset{\shortparallel}{p}}, |\alpha|) = 1 \Rightarrow \xi_p^{|\alpha|}$ is a primitive p-th complex root of 1.

Hence $\sum_{k=0}^{p-1} \xi_p^{k|\alpha|} = 0$; if $p \mid |\alpha|$, then $\rho(x^\alpha) = x^\alpha \Rightarrow$

$\mathbb{C}[x]^G$ is, as $\mathbb{C}$-algebra, generated by $\forall$ monomials of degree p. ▨

<u>Theorem 22</u>: (Molien's theorem) $G < GL(n,\mathbb{C})$ finite group, acting linearly on $R = \mathbb{C}[x]$. We denote $\mathbb{C}[x]^G_i$ the vector space generated by $\forall$ homogeneous invariants of degree $i \in \mathbb{N}$.

Put $$H(\mathbb{C}[x]^G, \lambda) := \sum_{i=0}^{\infty} \dim \mathbb{C}[x]^G_i \lambda^i. \quad \text{Then}$$

$$H(\mathbb{C}[x]^G, \lambda) = \frac{1}{|G|} \sum_{\tilde{g} \in G} \frac{1}{\det(Id - \lambda \tilde{g})}, \quad \tilde{g} \in GL(n,\mathbb{C}).$$

<u>Pf</u>: The Reynolds operator $\rho : R \to S = R^G$ is $\mathbb{C}$-linear $\Rightarrow \rho$ induces $\mathbb{C}$-linear map $\rho|_{R_i} = \rho_i : \underset{= \mathbb{C}[x]_i}{R_i} \to (R^G)_i$, with $(\ )_i \equiv i$-th degree/homogeneity elements. Thus $\operatorname{rank}(\rho_i) = \operatorname{tr}(\rho_i) = \dim(R^G)_i$, because ρ_i are projectors $\forall i \in \mathbb{N}$: $\rho_i^2 = \rho_i$, hence the eigenvalues of ρ_i are $\operatorname{Spec}(\rho_i) \in \{0,1\}$. This implies

$$H(R^G, \lambda) = \sum_{i=0}^{\infty} \dim(R^G)_i \lambda^i = \sum_{i=0}^{\infty} \operatorname{tr}(\rho_i) \lambda^i = \frac{1}{|G|} \sum_{\tilde{g} \in G} \sum_{i=0}^{\infty} \operatorname{tr}(\tilde{g}|_{R_i}) \lambda^i$$
$$= \frac{1}{|G|} \sum_{\tilde{g} \in G} \left(\sum_{i=0}^{\infty} \operatorname{tr}(\tilde{g}|_{R_i}) \lambda^i \right).$$

Now we prove: $$\sum_{i=0}^{\infty} \operatorname{tr}(\tilde{g}|_{R_i}) \lambda^i = \frac{1}{\det(Id - \lambda \tilde{g})}.$$

$\mathbb{C}$ is alg. closed & G is finite group $\Rightarrow$ $\forall \tilde{g} \in G$ can be diagonalized,
($\forall \tilde{g} \in G$ has finite order)

$x_1, \dots, x_n$ a basis of eigenvectors in $\mathbb{C}[x]_1$, $\lambda_1, \dots, \lambda_n$ their eigenvalues.
A basis of $\mathbb{C}[x]_i$ is given by $\forall$ monomials of degree i in $x_1, \dots, x_n$
$\Rightarrow$ eigenvalues of $\tilde{g}|_{R_i}$ are $\lambda^\alpha \equiv \lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n}$, $\alpha \equiv (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, $|\alpha| = i$, thus

$$\operatorname{tr} \tilde{g}|_{R_i} = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n, \sum \alpha_j = i} \lambda_1^{\alpha_1} \lambda_2^{\alpha_2} \cdots \lambda_n^{\alpha_n}, \quad \text{and so}$$

$$\sum_{i=0}^{\infty} \operatorname{tr} \tilde{g}|_{R_i} \lambda^i = \prod_{j=1}^{n} \frac{1}{(1-\lambda_j \cdot \lambda)} = \prod_{j=1}^{n} \frac{\lambda_j^{-1}}{(\lambda_j^{-1}-\lambda)} = \frac{\det \tilde{g}^{-1}}{\det(\tilde{g}^{-1}-\lambda \mathrm{Id})}$$

$$= \frac{1}{\det(\mathrm{Id}-\lambda\tilde{g})}, \text{ therefore}$$

$$H(\overset{S}{\overset{\shortparallel}{R^G}}, \lambda) = \frac{1}{|G|} \sum_{\tilde{g}\in G} \frac{1}{\det(\mathrm{Id}-\lambda\tilde{g})}. \quad ▨$$

<u>Example 23</u>: Consider the quaternion group Q_8 acting on $\mathbb{C}[x,y]$:

$$Q_8 = \left\{ \pm\begin{bmatrix}1&0\\0&1\end{bmatrix}, \pm\begin{bmatrix}i&0\\0&-i\end{bmatrix}, \pm\begin{bmatrix}0&1\\-1&0\end{bmatrix}, \pm\begin{bmatrix}0&i\\i&0\end{bmatrix} \right\} < GL(2,\mathbb{C})$$

To compute Molien's series, we have

$\tilde{g}$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$	$\begin{bmatrix}i&0\\0&-i\end{bmatrix}$	$\begin{bmatrix}-i&0\\0&i\end{bmatrix}$	$\begin{bmatrix}0&1\\-1&0\end{bmatrix}$	$\begin{bmatrix}0&-1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&i\\i&0\end{bmatrix}$	$\begin{bmatrix}0&-i\\-i&0\end{bmatrix}$
$\det(\mathrm{Id}-\lambda\tilde{g})$	$(1-\lambda)^2$	$(1+\lambda)^2$	$1+\lambda^2$	$1+\lambda^2$	$1+\lambda^2$	$1+\lambda^2$	$1+\lambda^2$	$1+\lambda^2$

$$\Rightarrow H(\mathbb{C}[x,y]^{Q_8}, \lambda) = \frac{1}{8}\left[\frac{1}{(1-\lambda)^2} + \frac{1}{(1+\lambda)^2} + \frac{6}{1+\lambda^2}\right] = \frac{1+\lambda^6}{(1-\lambda^4)^2}$$

$$= 1 + 2\lambda^4 + \lambda^6 + \dots$$

$\Rightarrow$ there are 2-invariants of degree 4 and one of degree 6.

The G-orbit of both $\overset{x_1}{\overset{\shortparallel}{x}}$ and $\overset{x_2}{\overset{\shortparallel}{y}}$ is $\{\pm x, \pm y, \pm ix, \pm iy\}$, hence

$$\rho(x^4) = \frac{1}{8}\left(x^4 + x^4 + y^4 + y^4 + x^4 + x^4 + y^4 + y^4\right) = \frac{1}{2}(x^4+y^4),$$

$\rho(x^2y^2) = x^2y^2$ $\quad$ (x^4+y^4 and x^2y^2 are lin. independ.)
$\Rightarrow$ basis of $\mathbb{C}[x,y]^{Q_8}_4$

$J =$ Jacobian : $f_1,\dots,f_n \in \mathbb{C}[x_1,\dots,x_n]$ and $\tilde{g} \in GL(n,\mathbb{C})$, by the chain rule $J(\tilde{g}f_1, \tilde{g}f_2, \dots, \tilde{g}f_n) = \det\tilde{g}^{-1} J(f_1,f_2,\dots,f_n)$; in the present case, $J(x^4+y^4, x^2y^2) = 8(x^5y - y^5x)$

$$\Rightarrow \left.\begin{array}{l}\alpha = x^4+y^4\\ \beta = x^2y^2\\ \gamma = x^5y-y^5x\end{array}\right\} \in \mathbb{C}[x,y]^{Q_8} \Rightarrow \mathbb{C}[\alpha,\beta,\gamma] \subseteq \mathbb{C}[x,y]^{Q_8}.$$

It is easy to check $\gamma^2 = \alpha^2\beta - 4\beta^3$:

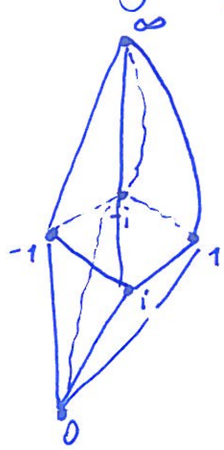
$$\mathbb{C}[\alpha,\beta,\gamma] \simeq \mathbb{C}[u,v,w]/\langle w^2+4v^3-u^2v\rangle$$

$\deg u = 4 = \deg v$
$\deg w = 6$
($\deg = 12$ relation)

$\Rightarrow \mathbb{C}[\alpha,\beta] \oplus \mathbb{C}[\alpha,\beta]\gamma \subseteq \mathbb{C}[x,y]^{Q_8}$ subring, but (!) the Molien's series is the same ($= \dfrac{1+\lambda^6}{(1-\lambda^4)^2}$), due to $\gamma^2 \in \mathbb{C}[\alpha,\beta]$)

$\Rightarrow$ the rings coincide : $\mathbb{C}[x,y]^{Q_8} \simeq \mathbb{C}[u,v,w]/\langle w^2+4v^3-u^2v\rangle$

Quaternion group Q_8 (of order 8) = binary dihedral group of the 2-gon : the zeroes of degree 6 invariant γ (viewed as pts on Riemann sphere), are the vertices of a regular octahedron



<u>Example 24</u> : The dihedral group $G = D_{12}$ has a representation in $GL(3,\mathbb{C})$,

$$G = \{\sigma^i\delta^j \mid i \in \{0,1\},\ j \in \{0,1,2,3,4,5\}\}$$

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},\quad \delta = \begin{pmatrix} 1/2 & -\sqrt{3}/2 & 0 \\ \sqrt{3}/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Find $M_G(\lambda)$ of $\mathbb{C}[x,y,z]^G$, analyze invariants & their degrees, Reynolds operator, etc.

<u>Example 25</u> : The dihedral group D_{2k} is the group of symmetries of a regular k-gon centered at the origin. It is given by $D_{2k} = \{r^i\rho^j \mid i \in \{0,1\},\ j \in \{1,2,\dots,k-1\}\}$, with

$$\rho = \begin{pmatrix} \cos 2\pi/k & -\sin 2\pi/k \\ \sin 2\pi/k & \cos 2\pi/k \end{pmatrix},\quad r = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

ρ diagonalizable with eigenvalues $\lambda = e^{2\pi i/k}$, $\lambda^{-1} = \bar{\lambda}$

$\Rightarrow \det(1-\rho' t) = (1-\lambda' t)(1-\lambda' t)$.

Find $H(\mathbb{C}[x,y]^{D_{2k}}, t) = ?$, analyze invariants, degrees, Reynolds operator, etc.

<u>Example 26</u>: $G = A_n$ alternating group, $A_n \leq S_n$ (even permutations)

$$\left\{ \begin{matrix} A_n - \text{invariant} \\ \text{polynom.} \end{matrix} \right\} \simeq \left\{ \begin{matrix} \text{symmetric} \\ \text{polyn.} \end{matrix} \right\} \oplus \left\{ \begin{matrix} \text{alternating} \\ \text{polyn.} \end{matrix} \right\},$$

free rank $= 1$ - module over symmetr. polyn., generated by $\Delta(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$.

Cohen-Macaulay property of invariant rings

$R_i \cdot R_j \subseteq R_{i+j}$

<u>Def 27</u>: Assume $R = \bigoplus_{d=0}^{\infty} R_d$ is a graded K-algebra over a field K s.t. $R_0 = K$. A set $f_1, \dots, f_r \in R$ of homog. elements is homogeneous system of parameters if

a/ $f_1, \dots, f_r$ ~~$\in K[V]^G$~~ are algebraically independent,

b/ R is a fin. gen. module over $K[f_1, \dots, f_r]$.

If $f_1, \dots, f_r \in K[V]^G$ is a homogeneous system of parameters, then $f_1, \dots, f_r$ are <u>primary</u> invariants. Then Hilbert's theorem implies

$$K[V]^G = K[f_1, \dots, f_r]\, g_1 + K[f_1, \dots, f_r]\, g_2 + \dots + K[f_1, \dots, f_r]\, g_s$$

with $g_1, \dots, g_s \in K[V]^G$ homogeneous, called <u>secondary</u> invariants.

If $R = \bigoplus_{d=0}^{\infty} R_d$ is a finitely generated graded algebra with $R_0 = K$, then R has a homogeneous system of parameters (in particular, invariant rings of finite or reductive algebraic groups have homogeneous systems of parameters)

Question: When is $K[V]^G$ free over $K[f_1, \dots, f_r]$?
($f_1, \dots, f_r \in K[V]^G$ primary invariants)

Def 28: R Noetherian ring, M a fin. gen. R-mod.

a/ $f_1,..,f_r \in R$ is M-regular if $M/(f_1,..,f_r)M \neq 0$, and $f_i : M/(f_1,..,f_{i-1})M \xrightarrow{f_i} M/(f_1,..,f_{i-1})M$ is injective for all $i=1,..,k$.

b/ $I \subseteq R$ an ideal, $I \cdot M \neq M$. Then the depth of I on M is the maximal length k of an M-regular sequence $f_1,..,f_k$ with $f_i \in I$; denoted by $\operatorname{depth}(I,M) = k$.

c/ If R is local or graded ring with maximal (homogeneous) ideal m, we write $\operatorname{depth}(M)$ for $\operatorname{depth}(m, M)$.

d/ If R is local Noetherian ring with max. ideal m, then M is Cohen-Macaulay if $\operatorname{depth}(M) = \dim(M)$, $\dim(M)$ is the Krull dimension of $R/\operatorname{Ann}_R(M)$. If R is not local, then M is C-M if $\forall$ maximal ideals $m \in \operatorname{Supp}(M)$ (i.e. m containing $\operatorname{Ann}_R(M)$), M_m is C-M as an R_m-module. (M_m, R_m localizations for m.)

e/ R is C-M if it is C-M as a module over itself.

A polynomial ring is C-M. Characterizations of C-M for graded algebr.:

Lemma 29: R Noeth. graded K-algebra, $R_0 = K$. Then TFAE:

a/ R is C-M ring.

b/ $\forall$ homog. system of parameters is R-regular.

c/ If $f_1,..,f_r$ is a homog. system of param., then R is a free module over $K[f_1,..,f_r]$.

d/ there is a homog. system of param. $f_1,..,f_r$ s.t. R is a free $K[f_1,..,f_r]$-module.

(14)

For example, for $R = K[x_1, \dots, x_n]$ a polynomial ring over K. If $S \subseteq R$ is a fin. gen. graded subalgebra with the property that $\forall\, I \subseteq S$ ideal, $IR \cap S = I$. Then S is C-M ring.

We remark that the existence of a homogeneous system of parameters is guaranteed by the Noether normalization theorem, but they are not unique (e.g., one can substitute any element in a homogeneous system of parameters by a power of itself.)

In the case of finite groups we have

Th 30: (Hochster, Eagon): If char(K) does not divide the order $|G|$ of finite group G, then $K[V]^G$ is C-M ring.

Example: We consider the permutation group G of order 4, generated by $(12)(34)$ and $(14)(23)$, and V is the 4-dim module over $K = \mathbb{Q}$ for G. Molien's formula gives

$$H(K[V]^G, t) = \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{3}{(1-t^2)^2}\right) =$$

$$= \frac{1+t^3}{(1-t)(1-t^2)^3}$$

$\Rightarrow$ $(1,2,2,2)$ are the smallest possible degrees for primary invariants. We find

$$f_1 = x_1 + x_2 + x_3 + x_4$$

$$f_2 = (x_1 - x_2 + x_3 - x_4)^2$$

$$f_3 = (x_1 - x_2 - x_3 + x_4)^2$$

$$f_4 = (x_1 + x_2 - x_3 - x_4)^2.$$

Prop 31: Denote $d_1, \dots, d_n$ degrees of primary invariants of a finite matrix group $G < GL(n, \mathbb{C})$. Then

a) the number of secondary invariants is $r = d_1 d_2 \dots d_n / |G|$, and

b) the degrees (together with multiplicities) of the secondary invariants are the exponents of the generating function

$$H(\mathbb{C}[x]^G, t) \cdot \prod_{i=1}^{n} (1 - t^{d_i}) = t^{e_1} + t^{e_2} + \dots + t^{e_r}.$$

Pf: By Molien's theorem,

$$H(\mathbb{C}[x]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(Id - gt)} = \frac{t^{e_1} + t^{e_2} + \dots + t^{e_r}}{\prod_{i=1}^{n} (1 - t^{d_i})}$$

and so

$$\frac{1}{|G|} \sum_{g \in G} \frac{(1-t)^n}{\det(Id - gt)} = \frac{t^{e_1} + t^{e_2} + \dots + t^{e_r}}{\prod_{i=1}^{n} (1 + t + t^2 + \dots + t^{d_i - 1})}.$$

The evaluation in $t = 1$ gives $\frac{r}{d_1 \cdot \ldots \cdot d_n}$ on the RHS, while on the LHS survives just $g = e$ and this gives $\frac{1}{|G|}$ (the other group elements $g \neq 0$ do not contribute.) ▨

The second formula is the consequence of the first.

Example 32: Consider the matrix group

$$G = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \right\} \leq GL(3, \mathbb{C}).$$

G is a cyclic group of order 4, the ring of invariants $\mathbb{C}[x_1, x_2, x_3]^G = S$ has Hilbert series

$$H(S,t) = \frac{1}{4}\left[\frac{1}{(1-t)^3} + \frac{2}{(1+t)(1+t^2)} + \frac{1}{(1+t)^2(1-t)}\right]$$

$$= \frac{1-t+t^2+t^3}{(1+t)^2(1+t^2)(1-t)^3} = 1+2t^2+2t^3+5t^4+4t^5+\ldots$$

and the polynomials

$$\left.\begin{aligned} \theta_1(x_1,x_2,x_3) &= x_1^2+x_2^2 \\ \theta_2(x_1,x_2,x_3) &= x_3^2 \\ \theta_3(x_1,x_2,x_3) &= x_1^4+x_2^4 \end{aligned}\right\} G\text{-invariants}$$

By Jacobi criterion, $\theta_1, \theta_2, \theta_3$ are algebraically independent, hence they are primary invariants. The number of secondary invariants is $\frac{(\deg\theta_1)(\deg\theta_2)(\deg\theta_3)}{4} = 4$, and their degrees are

$$H(\mathbb{C}[x]^G, t)(1-t^2)^2(1-t^4) = \left(\frac{1-t+t^2+t^3}{(1+t)^2(1+t^2)(1-t)^3}\right)\cdot(1-t^2)^2\cdot(1-t^4)$$

$$= 1+2t^3+t^4.$$

Hence $e_1=1$, $e_2=3=e_3$, $e_4=4$. The application of Reynolds operator gives the secondary invariants:

$\eta_1(x_1,x_2,x_3)=1$, $\eta_2(x_1,x_2,x_3)=x_1x_2x_3$, $\eta_3(x_1,x_2,x_3)=x_1^2x_3-x_2^2x_3$, $\eta_4(x_1,x_2,x_3) = x_1^3x_2 - x_1x_2^3$. It is then elementary to verify the Hironaka decomposition of $\mathbb{C}[x]^G$:

$$\mathbb{C}[x]^G = \bigoplus_{i=1}^{4} \mathbb{C}[\theta_1,\theta_2,\theta_3]\,\eta_i.$$

<u>Remark:</u> Assume we have n-homogeneous polynomials

$f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_m]$, $n \leq m$ (in our case, $m = n$ and we have polynomials (homogeneous) $\theta_1, \theta_2, \theta_3$. The Jacobian criterion: $f_1, \dots, f_n$ are alg. independent iff $df_1 \wedge df_2 \wedge \dots \wedge df_n \neq 0$ ($\Leftrightarrow$ one of the maximal minors of $\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j=1}^{n,m}$ is non-zero.)