The Fundamental Theorem of Invariant Theory

Will Traves

USNA Colloquium

15 NOV 2006

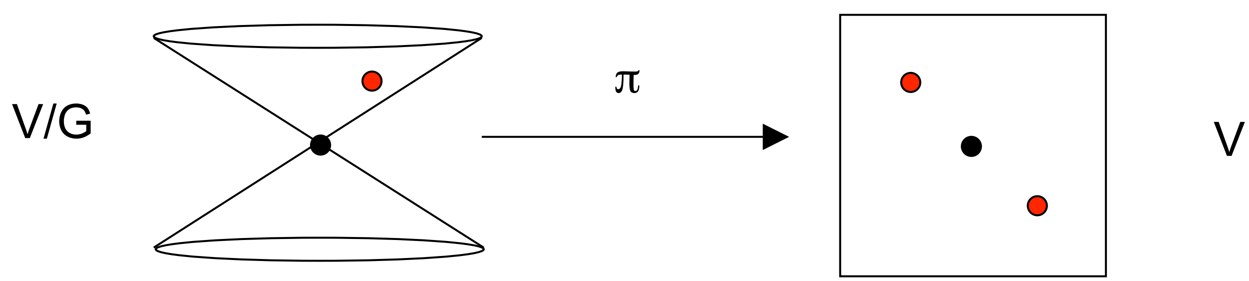
Invariant Theory

V: Complex n-dimensional vector space, C^n
G: group acting linearly on V

<u>Question</u>: How can we understand the quotient space V/G?

<u>Example</u>: $G = Z_2$ acting on $V = C^2$ via $(x,y) \rightarrow (-x, -y)$.
The ring of (polynomial) functions on V is C[V] = C[x,y].

The functions on V/G ought to be polynomials invariant under the action of G
$= C[V/G] = C[V]^G = \{ f(x,y): f(x,y) = f(-x,-y)\} = C[x^2, y^2, xy]$
$= C[X, Y, Z] / (XY-Z^2)$
$= C[X', Y', Z] / (X'^2 + Y'^2 - Z^2)$



Geometric Examples

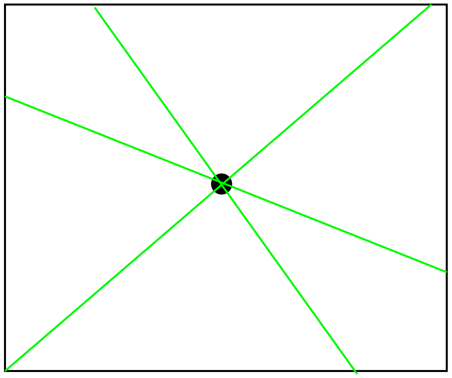
$G = C^*$ acts on $V = C^2$ via scaling

$g \bullet (x,y) = (gx, gy)$

$C[V]^G = C$ so $V//G$ is a point.

If we first remove the origin then we get

$V^* // G =$ **the projective line P^1**



In general, we need to remove a locus of bad points (**non-semi-stable points**) and only then quotient. This **GIT** quotient is useful in constructing moduli spaces.

<u>Example</u>: **moduli space of degree d rational plane curves**

Parameterization: $P^1 \to P^2$

$$[s: t] \to [F_1(s,t): F_2(s,t): F_3(s,t)]$$

So curves parameterized by P^{3d+2} but some of these are the same curve!

$$M = P^{3d+2} // PGL_2C.$$

This space is not compact; its compactification plays a key role in **string theory** and **enumerative geometry.**

Classical Invariant Theory

1800's: Many mathematicians (Cayley, Sylvester, Gordan, Clebsh, etc) worked hard to compute invariant functions (particularly of SL_2 actions).

1868: Gordan: $C[V]^{SL_2}$ is finitely generated (symbolic method)

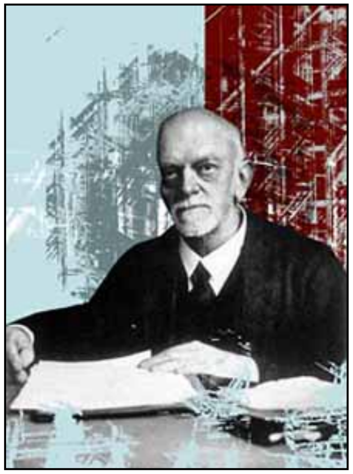
1890: **Hilbert's finiteness theorem**: $C[V]^G$ is finitely generated for a wide class of groups (linearly reductive groups)

Gordan: "Das ist Theologie und nicht Mathematik!"

1893: Hilbert makes his proof constructive.

1900: Hilbert asks whether $C[V]^G$ is always finitely generated. (Nagata: no)

P. Gordan



D. Hilbert

M. Nagata

The Reynolds Operator

If G acts on $V=C^2$ then G acts on R = C[V] = C[x,y] by $(g \bullet F)(x,y) = F(g^{-1} \bullet (x,y))$.
R^G = subring of R of functions F(x,y) such that $g \bullet F = F$.

The map $R^G \to R$ is an inclusion. **When is there a compatible projection back?**

G is **linearly reductive** if every G-invariant subspace W of V has a G-invariant complement:

$$V = W \oplus W^C$$

Examples are finite groups, C^*, SL_n, GL_n, O_n, etc.

Whenever G is linearly reductive, there is a splitting of $R^G \to R$: $R_d = R_d^G \oplus T$
The projection $R \to R^G$ is an R^G-linear map called the **Reynolds operator**.

When G is finite,

$$R(f) = \frac{1}{|G|} \sum_{g \in G} g \bullet f$$

Otherwise, the Reynolds operator is obtained by integration.

Hilbert's wonderful proof

Thm (Hilbert): If G is lin. reductive then R^G is f.g.

Proof: Consider the ideal $J = (F \in R^G_+)$ of R.

Hilbert's Basis Theorem says that the poly ring R is **Noetherian**, so every ideal in R is finitely generated. Let $F_1, \ldots, F_r$ be the generators of J.

We claim that $R^G = C[F_1, \ldots, F_r]$ and prove it by **induction** on degree. The degree zero pieces of both rings are C. Suppose that the two rings agree for degree d.

Let g be in R^G_d. Then g is in J and so for suitable G_i of degree d-deg(F_i) in R.

$$\boxed{g = G_1 F_1 + G_2 F_2 + \ldots + G_r F_r}$$

Now apply the Reynolds operator to get

$$\boxed{g = \mathbf{R}(g) = \mathbf{R}(G_1)F_1 + \ldots + \mathbf{R}(G_r)F_r}$$

But now each $R(G_i)$ is an invariant of degree less than d and so it is in $C[F_1, \ldots, F_r]$. Thus g is in $C[F_1,\ldots,F_r]$.

Derksen's Algorithm for R^G

Derksen modified Hilbert's constructive proof to give an algorithm to construct invariants.

To start, we parameterize the group G.

$$\Psi : G \times V \rightarrow V \times V \qquad \text{given by } \Psi(g,x) = (x, g \bullet x)$$

Let B = closure of the image of Ψ.

The variety B is cut out by equations in an ideal b that can be computed using Grobner bases (**eliminating the parameters** defining the group).

Hilbert-Mumford Criterion: $B \cap (X \times \{0\}) = V(\text{Hilbert ideal}) \times \{0\}$

Reynolds operator: $b + (z_1, \ldots, z_n) = \text{Hilbert ideal} + (z_1, \ldots, z_n)$

Derksen's algorithm: Compute b, set z's = 0, apply Reynolds operator to generators and get invariants generating the Hilbert ideal. These generate R^G.

Derksen's Algorithm for R^G

Harm Derksen and Gregor Kemper

Easy example

Let R=C[x,y,z] and G=Z_2.
Let G act on R by σ(x) = -x, σ(y)=z, σ(z) = y.

We represent G as **V**(t^2-1) and the action

$$\rho(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } \rho(-1) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

by the interpolation matrix

$$\rho(t) = \begin{bmatrix} t & 0 & 0 \\ 0 & \frac{t+1}{2} & \frac{1-t}{2} \\ 0 & \frac{1-t}{2} & \frac{t+1}{2} \end{bmatrix}$$

Easy example continued

$$\rho(t) = \begin{bmatrix} t & 0 & 0 \\ 0 & \frac{t+1}{2} & \frac{1-t}{2} \\ 0 & \frac{1-t}{2} & \frac{t+1}{2} \end{bmatrix} \Rightarrow$$

$t \bullet x = tx$

$t \bullet y = (t+1)y/2 + (1-t)z/2$

$t \bullet z = (1-t)y/2 + (1+t)z/2$

The ideal defining the graph of $\psi : \mathrm{G} \times \mathrm{X} \to \mathrm{X} \times \mathrm{X}$ is

β = $(t^2 - 1,\ z_1 - t\bullet x,\ z_2 - t\bullet y,\ z_3 - t\bullet z) \subset C[t,x,y,z,z_1, z_2, z_3]$

Compute the elimination ideal **b** = **β** $\cap$ $C[x,y,z, z_1, z_2, z_3]$ and set $z_1 = z_2 = z_3 = 0$ to get $(y+z, z^2, xz, x^2)$.

Applying the Reynolds operator **R**(f)=[f(x,y,z)+f(-x,z,y)]/2 gives gens for $\mathbf{R}^{\mathbf{G}}$: $y+z$, y^2+z^2, $xz-xy$, and x^2.

Grassmann Varieties

One of the most important moduli spaces in algebraic geometry is the space parameterizing the collection of k-planes in n-space.

Projectively this becomes the space of k-1 dimensional planes in n-1 dimensional space, **G**(k-1,n-1).

Each subspace is determined by a basis:

$$\begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ v_1 & v_2 & \cdots & v_k \\ \downarrow & \downarrow & & \downarrow \end{bmatrix}$$

Of course, there are many bases for each subspace. The group SL_kC acts on the basis M via change of coordiantes: $g \bullet M_v = M_{g \bullet v}$.

The projectivization of the quotient $M_{kxn} // SL_nC$ is the Grassmann variety **G**(k-1,n-1).

The Fundamental Theorem

The **first fundamental theorem of invariant theory** concerns the generators of the ring of invariants for **G**(k-1,n-1).

In small examples we could compute these using Derksen's algorithm.

THM: The generators for **G**(k-1,n-1) – the functions on the k x n matrices that are SL_k invariant – are the **Plucker coordinates**, the determinants of the various k x k minors.

$$\boxed{[jk] = x_{j1}x_{k2} - x_{k1}x_{j2} = \text{det of } j^{th} \text{ and } k^{th} \text{ columns}}$$

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \end{bmatrix}$$

For **G**(1,3) the 6 invariants satisfy a single relation, the Plucker relation

[12][34] – [13][24] + [14][23] = 0

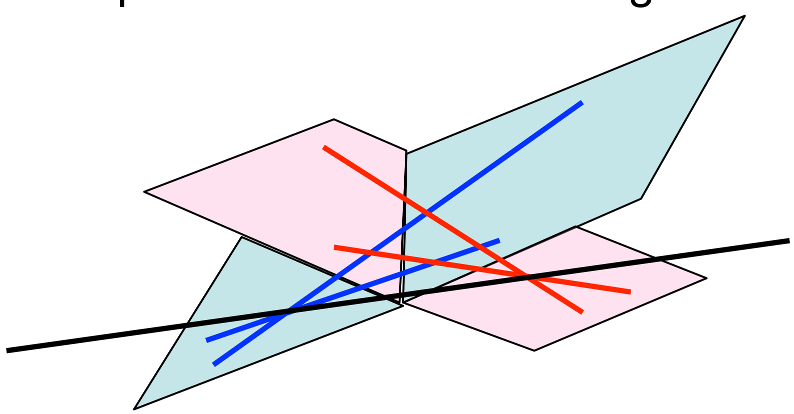
Schubert Calculus

Question: How many lines meet 4 given (general) lines in 3-space?

We'll solve this by looking at the moduli space **G**(1,3).

It is not hard to see that each of the conditions (that our line meet a given line) is a linear constraint in the Plucker coordinates.

The space **G**(1,3) sits inside $\mathbf{P}^5$ as a quadratic hypersurface. The four linear conditions cut out a line that meets **G**(1,3) in 2 points. These two points correspond to two lines meeting all four given lines!



Group actions on the Weyl algebra

Idea: replace R=C[**x**] with D(R)=C<**x**,$\partial_{\mathbf{x}}$> and compute **D(R)^G** = C<**x**,$\partial_{\mathbf{x}}$>^{G}.

Extending the group action: G acts on an operator $\theta \in D(R)$ by

$$\boxed{(g\bullet\theta)(f) = g \bullet (\theta(g^{-1} \bullet f)).}$$

Concretely, if g acts on $x_1,\ldots,x_n$ by the matrix **A** then g acts on $\partial_1,\ldots,\partial_n$ by the matrix **$(A^T)^{-1}$**.

This action preserves the **defining relations** on the Weyl algebra: $\left[\partial_i, x_j\right] = \partial_i x_j - x_j \partial_i = \delta_{ij}$

Sabbatical Work

The ring D(R) is **filtered** by the order of the differential operators.
The **associated graded** ring GrD(R) is a polynomial ring in 2n variables.

$[GrD(R)]^G = Gr[D(R)^G]$ so can use Derksen's algorithm to compute $Gr[D(R)^G]$.
The generators and relations on the graded ring can be **lifted** to give generators and relations for $D(R)^G$. I've done this for the case when $R = C[M_{k \times n}]$ and $G = SL_k C$, giving a **Fundamental Theorem of invariant theory for the Weyl algebra**.

There is a subtle distinction between the invariant differential operators and the differential operators on the quotient variety. There is a map

$$\boxed{\text{Invariant diff ops } D(R)^G \rightarrow \text{Diff ops on the quotient } D(R^G)}$$

and the kernel can be very hard to compute explicitly. I managed to do this for **G**(1,3), where the kernel is generated by the **Casimir operator**. This allowed me to give a complete presentation of the ring of differential operators on the Grassmann variety **G**(1,3).