Rings of invariants

Winfried Bruns

FB Mathematik/Informatik
Universität Osnabrück

wbruns@uos.de

Ann Arbor, August 1, 2008

This file contains my lecture at the conference celebrating Mel Hochster's 65th birthday. It surveys his work in invariant theory and work by others related to it.

References (except for the modular case discussed at the very end) can be found in Jürgen Herzog's and my book *Cohen-Macaulay rings*, revised edition (Cambridge University Press 1998). Its Chapter 6 covers most of the invariant theoretic results presented, and a proof of the theorem of Hochster and Huneke on direct summands of regular rings can be found in Chapter 10. Determinantal rings are discussed in Chapter 7; see also Udo Vetter's and my book *Determinantal rings*, Springer Lecture Notes 1327 (1988).

Winfried Bruns

Symmetric polynomials

Consider a polynomial $f = f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$, a permutation $\pi \in S_n$, and set

$$f^\pi = f(X_{\pi(1)}, \dots X_{\pi(n)}).$$

We call f symmetric if $f^\pi = f$ for all $\pi \in S_n$.

Theorem

The subalgebra of the symmetric polynomials is generated over K by the elementary symmetric functions

$$\varepsilon_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k}, \qquad k = 1, \dots, n,$$

and these are algebraically independent over K.

Linear transformations

Let K be a field and $R = K[X_1, \dots, X_n]$ the polynomial ring in n indeterminates.
The group $\mathrm{GL}(n, K)$ of invertible $n \times n$-matrices acts on R by linear transformations:
for $g \in \mathrm{GL}(n, K)$, $g = (a_{ij})$, and $f \in R$ set

$$f^g = f(X'_1, \dots, X'_n), \qquad X'_j = \sum_i a_{ij} X_i.$$

"We are led to essentially new and deep properties of forms through the application of linear transformations." (Hilbert, Lectures on invariant theory, 1893)

Note: $f \mapsto f^g$ is a K-algebra automorphism of R.

Invariants

Let $G \subset \mathrm{GL}(n, K)$ be a subgroup.

Definition

f is a G-invariant if $f^g = f$ for all $g \in G$.

$$R^G = \{f : f^g = f \text{ for all } g \in G\}$$

is the ring of G-invariants.

Standing assumption when we discuss R^G:

K is a field, $G \subset \mathrm{GL}(n, K)$ acts on $R = K[X_1, \dots, X_n]$ as above.

Clearly, $S = R^G$ is a graded ring: f is invariant $\iff$ its homogeneous components are invariant. Therefore

$$S = \bigoplus_{i=0}^{\infty} S_i$$

where S_i is the vector space of homogeneous invariants of degree i.

Basic questions of invariant theory

Following Hochster, Invariant theory of commutative rings, we ask:

- Under what conditions on G is R^G finitely generated as a K-algebra?
- When R^G is finitely generated, what are the generators and relations of R^G?
- What "good" properties does R^G enjoy?

Good properties: Cohen-Macaulay, Gorenstein, regular, factorial,...

Basic observation:

Proposition

R^G is a normal ring.

In fact, $R^G = \mathrm{QF}(R^G) \cap R$.

Linearly reductive groups

A linear representation of a group G over a field K is a homomorphism $\varphi : G \to \mathrm{GL}(V)$ for some K-vector space V. A subspace of V closed under the induced action of G is a G-module.

Definition

G is linearly reductive (over K) if every G-submodule U of a finite dimensional linear representation V has a G-module complement U'.

Examples of linearly reductive groups:

- G finite, $\operatorname{char} K \nmid |G|$
- the classical groups $\mathrm{GL}(n, K)$, $\mathrm{SL}(n, K)$ etc. in characteristic 0
- the algebraic torus $\mathrm{Diag}(n, K) \cong \mathrm{GL}(1, K)^n$ in all characteristics

The Reynolds operator

Suppose G is linearly reductive. Then V has a unique decomposition $V = V^G \oplus V'$ in which V^G is the subspace of all G-stable elements and V' is the sum of all simple G-modules on which G acts nontrivially.

Definition

The unique linear map $\rho : V \to V^G$ with $\rho|V^G = \mathrm{id}$ and $\rho|V' = 0$ is called the Reynolds operator.

For finite groups, the Reynolds operator is averaging over the orbit:

$$\rho(x) = \frac{1}{|G|} \sum_{g \in G} x^g.$$

The direct summand property

Clearly we also have a Reynolds operator for direct sums (and filtered direct limits) of finite-dimensional representations.

Proposition

Let $G \subset \mathrm{GL}(n, K)$ be linearly reductive and $R = K[X_1, \ldots, X_n]$. Then the Reynolds operator $\rho : R \to R^G$ is an R^G-linear map. Thus

$$R = R^G \oplus \operatorname{Ker} \rho$$

is a decomposition of R^G-modules.

Hilbert's theorem

Theorem (Hilbert 1890)

Let G be a linearly reductive subgroup of $\mathrm{GL}(n,K)$ and $R = K[X_1,\dots,X_n]$. Then R^G is a finitely generated K-algebra.

Proof.

Let I be the ideal of R^G generated by all invariant forms of degree > 0. By Hilbert's basis theorem, $IR = Rg_1 + \dots + Rg_m$ with homogeneous $g_1,\dots,g_m \in I$.

Let $f \in R^G$ be a form of degree d. Then

$$f = r_1 g_1 + \dots + r_m g_m, \qquad r_i \in R.$$

Apply the Reynolds operator:

$$f = \rho(f) = s_1 g_1 + \dots + s_m g_m, \qquad s_i = \rho(r_i) \in R^G.$$

By induction on d we have $s_i \in K[g_1,\dots,g_m]$. □

Hilbert's theorem is not the last word on finite generation, as clearly exhibited by a famous theorem of E. Noether:

Theorem

Let G be a finite subgroup of $\mathrm{GL}(n, K)$. Then R^G is a finitely generated K-algebra.

Further exploration of the finiteness question would lead us to reductive groups, Nagata's theorem, Mumford's conjecture ...

However, Nagata's counterexample to Hilbert's 14th problem shows that R^G is not always finitely generated.

Cohen-Macaulay rings

Let $S = \bigoplus_{i=0}^{\infty} S_i$ be a graded, finitely generated K-algebra, $S_0 = K$. Then S has a homogeneous system of parameters (h.s.o.p.) $x_1, \dots, x_d$, $d = \dim S$ (Krull dimension): S is a finitely generated $K[x_1, \dots, x_d]$-module and $x_1, \dots, x_d$ are algebraically independent.

Proposition

The following are equivalent:

- *S is a free $K[x_1, \dots, x_d]$-module;*
- *$x_1, \dots, x_d$ is an S-sequence, i. e. x_i is not a zero divisor modulo $Sx_1 + \dots + Sx_{i-1}$, $i = 1, \dots, n$;*
- *every h.s.o.p. of S is an S-sequence.*

One calls S Cohen-Macaulay if it satisfies the conditions of the proposition.

Finite groups

Theorem (Grauert-Remmert-Riemenschneider, Hochster-Eagon 1971)

Let $G \subset \mathrm{GL}(n, K)$ be a finite group of order not divisible by char K*. Then R^G is Cohen-Macaulay.*

Proof.

Set $S = R^G$. Let $x_1, \dots, x_n$ be a h.s.o.p. for $S \Rightarrow x_1, \dots, x_n$ is a h.s.o.p. for R (since $R : S$ is module finite), and therefore an R-sequence.
$yx_{i+1} \in Sx_1 + \cdots + Sx_i \Rightarrow y \in Rx_1 + \cdots + Rx_i$, and Hilbert's argument shows $y \in Sx_1 + \cdots + Sx_i$. □

Counterexample when char $K \mid |G|$: for a certain action of $G = \mathbb{Z}/4\mathbb{Z}$ on $R = (\mathbb{Z}/2\mathbb{Z})[X_1, \dots, X_4]$, the ring R^G is not Cohen-Macaulay, but factorial (Bertin, 1967, extension by Fossum and Griffith 1975).

Determinantal rings

Let A be a matrix with entries in a ring R. Then we set

$$I_t(A) = \text{ ideal generated by the } t\text{-minors of } A.$$

(A t-minor is the determinant of a $t \times t$ submatrix.)

Let $X = (X_{ij})$ be a matrix of indeterminates and
$K[X] = K[X_{ij} : i = 1, \dots, m, j = 1, \dots, n]$. We assume that $m \le n$.

Put $I_t = I_t(X)$ and $R_r = K[X]/I_{r+1}$.

Macaulay (1916): I_m is unmixed
Eagon-Northcott (1962): R_{m-1} Cohen-Macaulay normal domain
Sharpe (1965): ditto for R_1 (also done by Chow 1964)
Mount (1967): I_t prime for all t

Theorem (Hochster-Eagon 1971)

R_r is a Cohen-Macaulay normal domain for all r.

The proof uses the technique of principal radical systems, an induction over a huge system of ideals, accompanied by generic points, i. e, homomorphisms to polynomial rings with the universal property that homomorphisms into fields factor through them:

$$\begin{array}{ccc} S & \longrightarrow & K[Y] \\ & \searrow \quad \swarrow & \\ & L & \end{array}$$

The generic point of R_r itself makes it a ring of invariants in all characteristics (De Concini-Procesi 1976; char $K = 0$ Weyl 1939).

Consider an $m \times r$ matrix Y of indeterminates and an $r \times n$ matrix Z. Then rank $YZ = r$, and the substitution $X_{ij} \mapsto (YZ)_{ij}$ yields a homomorphism

$$\gamma : R_r \to K[Y;Z], \qquad \gamma(R_r) = K[YZ].$$

This is a generic point: every matrix A of rank $\le r$ over a field can be factored as a product of BC of matrices of formats $m \times r$, $r \times n$.

R_r a domain $\Rightarrow R_r \cong K[YZ]$, the algebra generated by the entries of YZ.

$\mathrm{GL}(r, K)$ acts on $K[Y;Z]$ by linear substitutions, namely

$$Y \mapsto YU, \quad Z \mapsto U^{-1}Z, \qquad U \in \mathrm{GL}(r, K),$$

entry by entry. Clearly $(YZ)^U = (YU^{-1})(UZ) = YZ$, and $K[YZ]$ consists of invariants.

Let $f(Y;Z)$ be invariant, homogeneous in Y of degree d.
Choose $r \times r$-submatrices Y' an of Y and Z' of Z.

$$f(Y;Z) = f(YZ'(Y'Z')^{-1}, Y'Z)$$
$$= f(YZ'\det(Y'Z')^{-1}\operatorname{Adj}(Y'Z'), Y'Z) = (\det Y'Z)^{-d} g,\ g \in K[YZ]$$

But $Y'Z'$ is an $r \times r$ submatrix of YZ. Varying Y' and Z' we see

$$f \cdot I_r(YZ)^d \subset K[YZ].$$

Normality $\Rightarrow$ $f \in K[YZ]$ since

$$\operatorname{ht} I_r(YZ)^d = \operatorname{ht} I_r/I_{r+1} \geq 2.$$

To sum up:

$$K[Y;Z]^{\mathrm{GL}(r,K)} = K[YZ] \cong R_r.$$

Related cases:

1. X a symmetric matrix, $K[X]/I_{r+1}(X)$, invariants of $O(r, K)$ (Kutz 1974)
2. X and alternating matrix, $K[X]/\operatorname{Pf}_{r+1}(X)$, invariants of $\operatorname{Sp}(r, K)$ (Marinov 1979; Kleppe and Laksov 1980)
3. coordinate rings of Grassmanians and their Schubert varieties (Musili 1971, Laksov 1972, Hochster 1973), $\operatorname{SL}(m, K)$ invariants of $K[X]$, X an $m \times n$ matrix of indeterminates under the action $X \mapsto UX$, $U \in \operatorname{SL}(m, K)$.

Characteristic free realization as invariant rings by De Concini and Procesi (1976), for (3) already by Igusa (1954).

Toric rings

Let $G \subset \mathrm{Diag}(n, K) \subset \mathrm{GL}(n, K)$ be a linearly reductive group of diagonal matrices. Equivalently, $G \cong \mathrm{Diag}(r, K) \times A$ where A is finite abelian with $|A|$ not divisible by char K. (Every simple G-module has dimension 1.)

Suppose $g \in G$ has diagonal entries $(d_1, \dots, d_n)$. Then

$$(X_1^{e_1} \cdots X_n^{e_n})^g = d_1^{e_1} \cdots d_n^{e_n} X_1^{e_1} \cdots X_n^{e_n}.$$

Thus $f = f^g \iff \mu^g = \mu$ for all monomials μ of f, and R^G is a normal subalgebra of R generated by finitely many monomials:

$$R^G = K[M], \qquad M \text{ a normal affine monoid (of monomials).}$$

Finite generation in this case follows also from Gordan's lemma.

Theorem (Hochster 1972)

A normal affine monoid algebra $K[M]$ is Cohen-Macaulay.

Normal affine monoids come up naturally in discrete polyhedral geometry, and the spectra of their algebras are the affine building blocks of toric varieties.

Hochster's proof makes use of the polyhedral geometry of affine monoids and uses the shellability of polytopes proved by Brugesser and Mani. A "shellable" system of ideals yields natural Mayer-Vietoris sequences from which Cohen-Macaulayness follows by induction.

A combinatorial application of Hochster's theorem is the nonnegativity of toric h-vectors.

The Hochster-Roberts theorem

Theorem (Hochster-Roberts 1974)

Let G be a linearly reductive group acting rationally on a noetherian regular K-algebra. Then R^G is Cohen-Macaulay.

The proof is a tour de force, using reduction to characteristic p and "involving fairly technical contortions".

A sharper version is proved in characteristic p:

Theorem

Let R be a noetherian regular K-algebra, char $K = p > 0$*, and S a subalgebra. If S is a direct S-summand of R, then S is Cohen-Macaulay.*

Actually, purity of the extension $S \to R$ would suffice (also in the theorems to follow).

Extensions of the Hochster-Roberts theorem

Theorem (Kempf 1980)

Let $S \subset R$ be an extension of finitely generated algebras over a field K. If R is regular and S is a direct summand of R, then S is Cohen-Macaulay.

For $R = K[X_1, \ldots, X_n]$ and a graded subalgebra S there exists a short proof by Knop.

Theorem (Boutot 1987)

Let $S \subset R$ be an extension of finitely generated algebras over a field K, $\operatorname{char} K = 0$. If R has rational singularities and S is a direct summand of R, then S has rational singularities, too.

Now we enter the territory of tight closure . . .

Theorem (Hochster-Huneke 1995)

Let R be a regular noetherian ring containing a field K and S a K-subalgebra. If S is a direct summand, then it is Cohen-Macaulay.

The canonical module and Gorenstein rings

Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a graded, finitely generated K-algebra, $R_0 = K$ with h.s.o.p. $x_1, \dots, x_d$. Set $S = K[x_1, \dots, x_d]$ and assume R is Cohen-Macaulay. Then

$$\omega_R = \operatorname{Hom}_S(R, S)$$

is called the canonical module of R. (We neglect the shift that is necessary for the correct grading.)

It is important that ω_R as an R-module does not depend on the choice of the h.s.o.p.

One calls R a Gorenstein ring if $R \cong \omega_R$ as an R-module.

Gorenstein rings enjoy especially good homological and combinatorial properties.

The canonical module of a ring of invariants

Let $G \subset \mathrm{GL}(n, K)$ as above act on $R[X_1, \dots, X_n]$. Then the module of semi-invariants of the inverse determinant character is

$$R^{\det^{-1}} = \{f \in R : f^g = (\det g)^{-1} f\}.$$

Theorem

$R^{\det^{-1}}$ is the canonical module of R^G in the following cases:

1. *(Watanabe) G is finite, $\operatorname{char} K \nmid |G|$;*
2. *(Danilov, Stanley) $G \subset \mathrm{Diag}(n, K)$. provided $R^{\det^{-1}} \neq 0$;*
3. *(B) determinantal rings.*

In particular, if $G \subset \mathrm{SL}(n, K)$ in (1) or (2), then R is Gorenstein.

Question: is $R^{\det^{-1}}$ always the canonical module, provided it is $\neq 0$? Intensively discussed by Hochster (1986). Negatively answered by Knop (1989).

Theorem (Knop 1989)

Let $G \subset \mathrm{GL}(n, K)$ be linearly reductive and set $G_v = \{g \in G : v^g = v\}$ for $v \in K^n$. If

$$\dim\{v \in K^n : |G_v| = \infty\} \leq n - 2$$

then $R^{\det^{-1}}$ is the canonical module of R.

The proof uses “the crowbar” (Knop).
Further work by Kac-Watanabe, Nakajima-Watanabe, Gordeev, Nakajima on the classification of actions of finite groups with complete intersection and hypersurface rings of invariants.

A classical result:

Theorem (Shephard-Todd, Chevalley, Serre)

Let $G \subset \mathrm{GL}(n, K)$ be a finite group, $\operatorname{char} K \nmid |G|$. *Then:*
R^G is regular $\iff$ G generated by pseudo-reflections

A pseudoreflection is a linear map π of finite order such that $\operatorname{rank}(\mathrm{id} - \pi \leq 1)$.

The modular case

If R is not Cohen-Macaulay, we can measure its deviation from the Cohen-Macaulay property in various ways.

Definition

Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a finitely generated graded K-algebra, $R_0 = K$. Then

$$\text{depth}\, R = \max\{n : x_1, \dots, x_n \text{ a hom. } R\text{-sequence}\}$$

The non-Cohen-Macaulay locus is given by

$$\text{NCM}(R) = \{\mathfrak{p} \in \operatorname{Spec} R : R_{\mathfrak{p}} \text{ not Cohen-Macaulay}\}$$

Clearly

$$R \text{ Cohen-Macaulay} \iff \text{depth}\, R = \dim R \iff \text{NCM}(R) = \emptyset$$

A general bound on depth:

Theorem (Ellingsrud-Skjelbred 1980)

Suppose char $K = p > 0$. *Let* $G \subset \mathrm{GL}(n, K)$ *be a finite group of order divisible by p. Then*

$$\operatorname{depth} R^G \geq \min(\dim V^P + 2, n) \quad \big(\geq \min(3, n)\big)$$

where P is the p-Sylow subgroup of G, with equality if $G = P$ *is a cyclic p-group.*

Theorem (Kemper 2000)

Let G be a finite group. If $\mathrm{NCM}(R^G) \neq \emptyset$, *then*

$$\dim \mathrm{NCM}(R^G) \geq 1.$$

In particular, if R^G is Buchsbaum, then it is Cohen-Macaulay.

The Shephard-Todd theorem cannot be generalized to the modular case, but one has:

Theorem (Dress 1969)

Let G be a finite group generated by pseudoreflections. Then R^G is a factorial ring.