ON POLYNOMIAL INVARIANTS

Walter Ferrer Santos   Gerardo Gonzalez-Sprinberg

ABSTRACT

Let S be a graded K-algebra equipped with a projection P into the kernel S^{Δ} of a family of homogeneous operators $\{\Delta_i{:}i{=}1,..,n\}$ of degree –1. In this paper we prove that under certain exactness hypothesis that relate the operators P and Δ_i, if S is a polynomial algebra so is S^{Δ}. We obtain additional information in the monomial case and show that the above result specialized to the case of a finite group generated by reflections produces a proof of the well known theorem of Chevalley, Shephard and Todd.

1. Introduction

In classical invariant theory , as described for example in (7), there were always considered "a first fundamental theorem" that produces the invariants, and a "second fundamental theorem" that yields the relationships between the invariants.

In the case of a finite group it has been known for a long time, that even for linear groups and their natural actions on the affine space, non trivial relations between the invariants may exist (see (6, Chapter 4 , Sect. 5) or (3)).

In these contexts it is natural to look for a characterization of the finite linear groups for which the fundamental invariants have no relations.

Around 1955, first in (5) by means of a case by case discussion, and then in (2) using a general method that we discuss at length along this paper, it was proved that a finite linear group over a field of characteristic zero is generated by reflections if and only if the algebra of its invariants is generated by algebraically independent elements.

The purpose of this paper is to use the standard machinery on graded algebras in order to prove a general theorem on kernels of homogeneous operators of degree –1, that yields –for the case of finite groups– the theorem of Chevalley, Shephard and Todd. The same methods applied to other situations produce analogous results on polynomial invariants.

Mots clés: polynomial invariants, reflection groups.

Classification AMS: 14L30, 13A50

2. Invariants of Graded Algebras

We assume that K is an arbitrary field and that all vector spaces we consider are defined over K. We consider objects graded over the semigroup N of natural numbers and if S is a graded algebra we assume that $S_0 = K$. We denote $S_+ = \sum_{n>0} S_n$.

We adopt the usual notation in the subject. For example if V and W are graded K–spaces, a linear map T is called homogeneous if there exists $d \in$ Z such that for all $n \in$ N, $T(V_n) \subset W_{n+d}$. The number d is called the degree of T. In this situation the subspace Ker(T) is graded and denoted as V^T.

In the case of a family of homogeneous operators $\mathcal{T} = \{T_\alpha : \alpha \in A\}$ we denote as $V^{\mathcal{T}} = V^{\{T_\alpha:\alpha\in A\}} = \bigcap_{\alpha\in A} V^{T_\alpha} = \bigcap_{\alpha\in A} \mathrm{Ker}(T_\alpha)$.

The theorem that follows is the starting point of our considerations. It can be considered as an abstraction of the basic techniques used in (2).

Theorem 2.1. *Let S be a graded commutative algebra without zero divisors and defined over K. Assume that there exist K-linear homogeneous operators $P, \Delta_1, \Delta_2, ..., \Delta_n : S \to S$ such that:*

(i) *The operators Δ_i are of degree -1, P is of degree 0 and $P(1) = 1$.*
(ii) *The operators Δ_i and P are S^Δ–linear, i.e., $\forall x \in S^\Delta, \forall y \in S$ we have $P(xy) = xP(y)$ and $\Delta_i(xy) = x\Delta_i(y)$. Here we abbreviate $\Delta = \{\Delta_1, .., \Delta_n\}$.*
(iii) *If for all $i = 1, 2, ..n$, $\mathcal{I} \subset S$ is a Δ_i-stable homogeneous ideal, then $\mathcal{I}$ is also P-stable and the sequence*

$$S/\mathcal{I} \xrightarrow{\widehat{P}} S/\mathcal{I} \xrightarrow{\widehat{\Delta_1}\oplus..\oplus\widehat{\Delta_n}} S/\mathcal{I} \oplus ... \oplus S/\mathcal{I}$$

is exact where $\widehat{P}, \widehat{\Delta_1}, .., \widehat{\Delta_n}$ are the corresponding maps defined on the quotient.

Then S is a free homogeneously generated S^Δ– module and $rk_{S^\Delta} S = dim_K S/S^\Delta_+ S$.

Proof: First we extract some consequences from our hypothesis and show that some of the statements in the theorem make sense. The K-space S^Δ is a graded K-subalgebra of S. If $x, y \in S^\Delta$, then $\Delta_i(xy) = x\Delta_i(y) = x.0 = 0$. Hence $xy \in S^\Delta$. Also as each of the Δ_i has degree -1, we have that $1 \in S^\Delta$. Suppose $x \in S^\Delta$, $P(x) = P(x.1) = xP(1) = x$. If we take $\mathcal{I} = 0$, the assertion (iii) implies that $\forall i = 1, .., n$, $\Delta_i P = 0$, i.e. $P(x) \in S^\Delta, \forall x \in S$, and hence P is a projection of S into the subalgebra S^Δ.

We write $S_+ = \oplus_{k>0} S_k$ and $S^\Delta_+ = \oplus_{k>0} S^\Delta_k$. Consider the ideal $S^\Delta_+ S = \mathcal{I}$ generated in S by S^Δ_+. Consider the K-space $S/\mathcal{I}$ and consider a family of homogeneous elements $\mathcal{B} = \{e_\alpha : \alpha \in A\}$ in S such that $\{e_\alpha + \mathcal{I} : \alpha \in A\}$ is a K-basis of $S/\mathcal{I}$. We prove that $\mathcal{B}$ is a family of free S^Δ–generators of S.

The proof that $\mathcal{B}$ generate S over S^Δ is standard. Call M the graded S^Δ–subalgebra of S generated by $\mathcal{B}$.

One proves by induction on $d \in$ N that $M_d = S_d$. To start with the induction we have to show that $M_0 = K$.

As $\{e_\alpha + \mathcal{I}\}$ generate $1 + \mathcal{I}$ over K, we can find scalars $a_\alpha \in K$ such that $1 - \sum_\alpha a_\alpha e_\alpha \in S^\Delta_+ S$. If we look at the degree zero part of the above equation we get

$1 - \sum_{\{\alpha:\deg(e_\alpha)=0\}} a_\alpha e_\alpha = 0$ so that for at least one α , $\deg(e_\alpha) = 0$. This implies that $M_0 = K$.

Suppose that we know that $\forall e < d$, $M_e = S_e$. If we take $f \in S_d$ we can find scalars a_α such that $f - \sum_\alpha a_\alpha e_\alpha \in \mathcal{I}$. We deduce that there exist homogeneous elements $r_\beta \in S_+^\Delta, f_\beta \in S$ such that $f - \sum_\alpha a_\alpha e_\alpha = \sum_\beta f_\beta r_\beta$. Taking the part of degree d of the above equation we obtain:

$$f - \sum_{\{\alpha:\deg(e_\alpha)=d\}} a_\alpha e_\alpha = \sum_{\{\beta:\deg(f_\beta)=d-\deg(r_\beta)\}} f_\beta r_\beta$$

As $\deg(r_\beta) > 0$, $d - \deg(r_\beta) = \deg(f_\beta) < d$. Hence $\forall \beta, f_\beta \in M$ and so does f.

Now we prove that $\mathcal{B}$ is free over S^Δ. The truth of this assertion will be deduced from the following: For any relation $x_1y_1+x_2y_2+...+x_my_m = 0$ with $x_i \in S^\Delta, y_i \in S$ and y_i homogeneous, we have $x_1 \in S^\Delta x_2 + .. + S^\Delta x_m$ or $y_1 \in S_+^\Delta S = \mathcal{I}$. Indeed, if we have a relation of the form $x_1e_1 + x_2e_2 + ... + x_me_m = 0$ with $x_i \in S^\Delta$, as $e_1 \notin \mathcal{I}$ we deduce that $x_1 = z_2x_2 + .. + z_mx_m$ with $z_2, ..., z_m \in S^\Delta$. Hence $(z_2x_2 + .. + z_mx_m)e_1 + ... + x_me_m = x_2(z_2e_1 + e_2) + .. + x_m(z_me_1 + e_m) = 0$. The alternative that $z_2e_1 + e_2 \in \mathcal{I}$ is impossible. This is because if $\deg(z_2) = 0$ the above equation produces a K-linear dependence relation between e_1 and e_2 in $S/\mathcal{I}$, and $\deg(z_2) > 0$ leads to the conclusion that $z_2e_1 \in \mathcal{I}$ and hence that $e_2 \in \mathcal{I}$. It follows then that $x_2 \in S^\Delta x_3 + .. + S^\Delta x_m$. Continuing in this way until the end we find a relation of the form $(t_1e_1 + ... + t_{m-1}e_{m-1} + e_m)x_m = 0$ with $t_i \in S^\Delta$. From this we conclude that $t_1e_1 + ... + t_{m-1}e_{m-1} + e_m = 0$. If we write $t_i = s_i + p_i$ being s_i and p_i the parts of degree zero and positive degree of t_i, we obtain a relation of the form $s_1e_1 + ... + s_{m-1}e_{m-1} + e_m \in S_+^\Delta S$. This contradicts the K-independence of the e_i modulo $S_+^\Delta S$.

All that remains to be done is to prove that the mentioned alternative is valid, i.e. that for any relation $x_1y_1 + x_2y_2 + ... + x_my_m = 0$ with $x_i \in S^\Delta, y_i \in S$ we have $x_1 \in S^\Delta x_2 + .. + S^\Delta x_m$ or $y_1 \in S_+^\Delta S = \mathcal{I}$.

The proof proceeds by induction on the degree of y_1.

If $y_1 = 0$ there is nothing to prove, and if $y_1 \in K^*$, we write $x_1 = x_2z_2 + .. + x_mz_m$. Applying P to the above equation we have $x_1 = P(x_1) = x_2P(z_2) + .. + x_mP(z_m)$. Hence $x_1 \in S^\Delta x_2 + .. + S^\Delta x_m$.

Suppose that $\deg(y_1) = d > 0$ and that the assertion is established for all elements of smaller degree.

If we apply the operator Δ_i to the original relation we get: $x_1\Delta_i(y_1) + x_2\Delta_i(y_2) + ... + x_m\Delta_i(y_m) = 0$. If $\Delta_i(y_1) = 0$ for all i, as y_1 has positive degree it belongs to S_+^Δ and we are done.

If for some i, $\Delta_i(y_1) \neq 0$, as this element has degree $d - 1$ we conclude–by induction– that we are in the hypothesis in which the alternative is true. Hence $x_1 \in S^\Delta x_2 + .. + S^\Delta x_m$ or $\Delta_i(y_1) \in S_+^\Delta S$ for all $i = 1, .., n$.

In the first case we are done so we can assume that for all i, $\Delta_i(y_1) \in S_+^\Delta S$.

Consider the exact sequence

$$S/S_+^\Delta S \xrightarrow{\widehat{P}} S/S_+^\Delta S \xrightarrow{\widehat{\Delta_1} \oplus .. \oplus \widehat{\Delta_n}} S/S_+^\Delta S \oplus .. \oplus S/S_+^\Delta S$$

The element $\overline{y_1} = y_1 + S^{\Delta}_{+}S \in \mathrm{Ker}(\widehat{\Delta_1} \oplus .. \oplus \widehat{\Delta_n})$, so that $\overline{y_1} \in \mathrm{Im}(\widehat{P})$,i.e., $P(y_1) - y_1 \in S^{\Delta}_{+}S$. But $y_1 \in S_+$ hence $P(y_1) \in S^{\Delta}_{+}S$. So that $y_1 \in S^{\Delta}_{+}S$.

□

3. Polynomial subalgebras of polynomial algebras

In the last section we proved that –under convenient hypothesis– the algebra S –considered as a module over the subalgebra S^{Δ}– is freely generated by homogeneous elements. In this situation standard results in commutative algebra–due mainly to J.P. Serre– guarantee that if S is a polynomial algebra so is S^{Δ}, see (4) . It is worth noticing that the above result is characteristic free. For the sake of completness we sketch its proof. By Serre's result mentioned above it is enough to prove that S^{Δ} has finite global dimension. We call n the number of free generators of S and take a proyective resolution of S^{Δ} of length $n-1$ and call Z its last kernel. We need to prove that Z is proyective. The freeness hypothesis and the fact that S is a polynomial algebra imply that the module induced at the level of S by Z, i.e. the module $Z \otimes_{S^{\Delta}} S$ is S-proyective. Using again the freenes of the extension on can prove that Z is also proyective as an S^{Δ}-module.

In the literature an elementary proof of the above result is usually presented –see for example (1) or (6)–. The price to be paid for being elementary is that it is not characteristic free.

We state and prove a couple of lemmas that seem to be a simplification of some of the arguments presented in the mentioned references and at the end produce the elementary proof.

Lemma 3.1. *Let K be an arbitrary field and let $R \subset S$ be a graded extension of commutative K-algebras. Assume also that:*

(i) *The extension $R \subset S$ is integral and flat.*
(ii) *If $\mathcal{I}$ is an arbitrary homogeneous ideal of R, then: $\mathcal{I}S \cap R = \mathcal{I}$.*
(iii) *If we order the family of all sets of homogeneous generators of the ideal R_+ of R in terms of their cardinal, there exists a minimal set in this family all whose elements have degrees non divisible by the characteristic exponent of K.*

Then, if S is a polynomial algebra generated by elements of degree one, R is a polynomial algebra with the same number of generators than S.

Proof: First recall that in the situation above the condition that S is integral over R is equivalent to the condition that S is finitely generated as an R–module and each of them implies that R is a finitely generated K-algebra. Hence R is noetherian and its fundamental ideal R_+ is finitely generated as an R-module.

Assume that $\mathcal{F} = \{f_1, .., f_m\}$ is a set of homogeneous generators as the in hypothesis (iii), i.e., such that the characteristic exponent of K does not divide $d_i = \deg(f_i)$.

An easy argument – that apparently goes back to Hilbert – guarantees that $\mathcal{F}$ generates R as a K-algebra.

We want to prove that $\mathcal{F}$ is algebraically independent over K.

Assume there is a non-zero polynomial $h \in K[X_1,..,X_m]$ such that $h(f_1,..,f_m) = 0$. We can assume that h is homogeneous in its variables and with minimal degree.

If we take the partial derivatives $h_i = \partial h/\partial X_i$ and consider $h_i(f_1,..,f_m) \in R$, we can define the ideal J of R as $J = \langle h_1(f_1,..,f_m),..,h_m(f_1,..,f_m)\rangle_R$.

From the hypothesis on the minimality of the degree of h we deduce that at least one of the generators $h_i(f_1,..,f_m), i = 1,..m$ of the ideal J is non-zero.

After renomination of variables one can define a number $s, 1 \le s \le m$ such that is minimal with respect to the property that

$$J = \langle h_1(f_1,..,f_m),..,h_s(f_1,..,f_m)\rangle_R$$

Hence, for all $s+1 \le j \le m$ we have that $h_j(f_1,..,f_m) = \sum_{i=1}^s r_{i,j} h_i(f_1,..,f_m)$ for some $r_{i,j} \in R$.

If we differentiate the equality $h(f_1,..,f_m) = 0$ with respect to the variables $T_l, l = 1,..,n$ and call $\partial f_i/\partial T_l = f_{i,l}$ we have: $0 = \partial/\partial T_l(h(f_1,..,f_m)) = \sum_{i=1}^m h_i(f_1,..,f_m)f_{i,l} =$
$\sum_{i=1}^s h_i(f_1,..,f_m)f_{i,l} + \sum_{j=s+1}^m (\sum_{i=1}^s r_{i,j} h_i(f_1,..,f_m))f_{j,l} =$
$\sum_{i=1}^s h_i(f_1,..,f_m)[f_{i,l} + \sum_{j=s+1}^m r_{i,j} f_{j,l}]$.

Now we prove that the term between brackets of the above equation belongs to the ideal R_+S.

Consider the R–linear map $\phi : R^s \to R$ given by the formula: $\phi(r_1,..,r_s) = \sum_{i=1}^s h_i(f_1,..,f_m)r_i$, and call $\phi_S : S^s \to S$ its extension to S^s by the same formula.

By definition $J = \mathrm{Im}(\phi)$. The hypothesis about the flatness of S as an R–module guarantees that the sequence:

$$0 \to \mathrm{Ker}(\phi) \to R^s \xrightarrow{\phi} J \to 0$$

remains exact after tensoring with S.

From the exactness of the tensored exact sequence

$$0 \to \mathrm{Ker}(\phi)S \longrightarrow S^s \xrightarrow{\phi_S} JS \to 0$$

we conclude that $\mathrm{Ker}(\phi_S) = \mathrm{Ker}(\phi)S$.

As we proved before the element
$f_{i,l} + \sum_{j=s+1}^m r_{i,j} f_{j,l} \in \mathrm{Ker}(\phi_S) = \mathrm{Ker}(\phi)S$.

Now we prove that $\mathrm{Ker}(\phi) \subset R_+$.

Consider a family of elements $(r_1,...,r_s) \in R^s : \sum_{i=1}^s h_i(f_1,..,f_m)r_i = 0$. The non-zero r_i that verify the above equation have part of degree zero equal to zero. Otherwise we would have a relation of the form $\sum_{i=1}^s h_i(f_1,..,f_m)\lambda_i = 0$ with some non-zero escalar coefficients $\lambda_i \in K$. This contradicts the minimality of the number of generators of the ideal J.

We conclude that for $1 \le i \le s, 1 \le l \le n, f_{i,l} + \sum_{j=s+1}^m r_{i,j} f_{j,l} \in R_+S$. Hence, as we know that the elements $\{f_1,..,f_m\}$ generate R_+, we conclude that there exist elements $s_{i,l,j} \in S,\ 1 \le j \le m$ such that for all $1 \le i \le s, 1 \le l \le n$,

$$f_{i,l} + \sum_{j=s+1}^m r_{i,j} f_{j,l} = \sum_{j=1}^m s_{i,l,j} f_j \qquad (1)$$

By Euler's relation we have that for all $1 \le i \le m,\ d_i f_i = \sum_{l=1}^n T_l f_{i,l}$.

Multiplying in equation 1 both sides by T_l and adding all the terms we obtain, for $1 \leq i \leq s$, $\sum_{l=1}^{n} T_l f_{i,l} + \sum_{j=s+1}^{m} r_{i,j}(\sum_{l=1}^{n} T_l f_{j,l}) = \sum_{j=1}^{m}(\sum_{l=1}^{n} T_l s_{i,l,j}) f_j$. If we call $t_{i,j} = \sum_{l=1}^{n} T_l s_{i,l,j}$ it is clear that $t_{i,j} \in S_+$ and that for $1 \leq i \leq s, d_i f_i + \sum_{j=s+1}^{m} r_{i,j} d_j f_j = \sum_{j=1}^{s} t_{i,j} f_j + \sum_{j=s+1}^{m} t_{i,j} f_j$.

We can rewrite the above equation as : $d_i f_i - \sum_{j=1}^{s} t_{i,j} f_j = \sum_{j=s+1}^{m}(t_{i,j} - d_j r_{i,j}) f_j$ and it is valid for $1 \leq i \leq s$.

Now we take for example $i = 1$ and display the equation above as: $d_1 f_1 - t_{1,1} f_1 - t_{1,2} f_2 - .. - t_{1,s} f_s = (t_{1,s+1} - d_{s+1} r_{1,s+1}) f_{s+1} + .. + (t_{1,m} - d_m r_{1,m}) f_m$. As the term $t_{1,1} f_1$ has no homogeneous part of degree d_1 when we take the homogeneous part precisely that degree of the displayed equation we obtain a relation of the form: $d_1 f_1 \in S f_2 + .. + S f_m$.

Using our hypothesis about the degrees of the polynomials f_i and calling $\mathcal{I}$ the R–ideal generated by $\{f_2, .., f_m\}$, we conclude that $f_1 \in \mathcal{I}S \cap R = \mathcal{I}$. Hence $f_1 \in Rf_2 + .. + Rf_m$ and this contradicts the minimality of the chosen set $\{f_i : i = 1, .., m\}$ of generators of R_+.

To prove the last assertion of the Lemma we consider the field extension $[R] \subset [S]$ that is algebraic because of hypothesis (i). Hence the transcendence degree of $[R]$ and of $[S]$ over the base field K are the same. Hence $m = n$.

□

Observe that in the case that the base field is of characteristic zero, the hypothesis (iii) about the degrees of the generators is authomatically verified.

The following Lemma guarantees that in the case that S is free homogeneous and finitely generated as an R-module the hypothesis (i) and (ii) are verified.

Lemma 3.2. *Let K be an arbitrary field and let $R \subset S$ be a graded extension of K-algebras. Assume that as an R–module , S has a finite basis of homogeneous elements, then the extension $R \subset S$ is integral and flat and for all homogeneous ideals $\mathcal{I}$ of R, $\mathcal{I}S \cap R = \mathcal{I}$.*

Proof: It is clear that being free and finite the extension has to be flat and integral.

We prove now the condition about the extension and contraction of ideals. Call $\{s_1, .., s_r\}$ an homogeneous finite basis of S over R. The neutral element can be written as $1 = a_1 s_1 + .. + a_r s_r$ with $a_i \in R$, hence it is clear that one of the s_i has degree zero and that the homogeneous basis can be taken of the form $\{1, .., s_r\}$.

Assume that $\mathcal{I}$ is an ideal of R and take $\xi \in \mathcal{I}S \cap R$. If we write $\xi = \sum a_j t_j$ with $a_j \in \mathcal{I}$ and $t_j \in S$ and $t_j = \sum b_{i,j} s_i$ with $b_{i,j} \in R$, we have a relation of the form $\xi = \sum_i (\sum_j a_j b_{i,j}) s_i$. As $\xi \in R$ we can also write $\xi = \xi 1 = (\sum_j a_j b_{1,j}) 1 + \sum_{i>1} (\sum_j a_j b_{i,j}) s_i$. Hence $\xi = (\sum_j a_j b_{1,j}) \in \mathcal{I}$.

□

4. The monomial case

In the monomial case additional information can be obtained. In fact , assume that $R \subset S$ is an extension of graded rings such that S is polynomial over K and free finitely generated as an R-module. Next theorem proves that in the case that

R is generated by monomials these monomials can be taken as powers of a system of variables of S.

Theorem 4.1. *Let K be an arbitrary field and let $R \subset S$ be a graded extension of K-algebras. Assume that S is polynomial algebra generated by elements $\{T_1, .., T_n\}$ of degree 1 and that R, as a K–algebra, is generated by monomials. Suppose that as an R-module S is finitely generated and free. Then:*

(i) *As R-module S has a finite monomial basis.*
(ii) *R is of the form $R = K[T_1^{d_1}, .., T_n^{d_n}]$.*

Proof: First we prove (i) i.e., we find a monomial R–basis of S. Let $\mathcal{B} = \{p_1, .., p_k\}$ be an arbitrary R–basis of S. To obtain a monomial basis we will perform on $\mathcal{B}$ elementary operations over R.

It is clear that at least one of the p_i has a non zero constant term, that we can assume to be equal to 1. By elementary operations over K we can transform the given basis into another–that will still be denoted as $\{p_1, .., p_k\}$– such that there is only one element of it , that we call p_1 that has a non zero constant term– and that we assume it is 1–. We can write $1 = p_1 + \sum_{i\geq 2} r_i p_i$ with $r_i \in R, 2 \leq i \leq k$. This equation defines an elementary transformation of the basis. Hence we can assume that $p_1 = 1$ and that the other p_i's have zero constant term.

Having settled the first step we proceed by induction. We assume $k > 1$ because if $k = 1$ we are done. We prove by induction in j that for all $1 \leq j \leq k$ we can find a basis $\{p_1, .., p_k\}$ of S over R such that:

(1) The element p_i is a monomial for $1 \leq i \leq j$.
(2) $\deg(p_1) < \deg(p_2) \leq .. \leq \deg(p_j)$.
(3) $\deg(p_j) \leq \deg(\mathrm{pf}(p_t)), \forall t > j$, where $\mathrm{pf}(p_t)$ denotes the principal form of the polynomial p_t.
(4) For all $t > j$ there is no monomial term in p_t of the form rp_i with r a monomial in R and $1 \leq i \leq j$.

Choose $h > j$ such that the term p_h has degree of its principal form minimal, and choose in p_h a monomial m_h of this degree. By elementary operations on $\mathcal{B}$ we may assume that no K–multiple of m_h is a monomial term of $p_{h'}$ for $h' \neq h, h' > j$. As $m_h \in S$, it can be written as $m_h = \sum_{l=1}^{n} r_l p_l$. From the above conditions we conclude that $r_l = 0, 1 \leq l \leq j$ and $r_h = 1$. After renumbering we may assume that $h = j+1$. Hence the substitution of p_h by m_h is an elementary transformation and after performing this transformation we see that conditions (1), (2) and (3) are verified for $h = j + 1$. Condition (4) can be obtained by elementary operations. Hence we obtain a monomial R–basis of S.

Now we prove (ii). Let $\mathcal{F} = \{f_j = \prod_{i=1}^{n} T_i^{u_{i,j}}, 1 \leq j \leq m\}$ be a monomial generating system of R_+. First we prove that for any $1 \leq i \leq n$ any system $\mathcal{F}$ as above contains a pure monomial of the form $T_i^{d_i}$ for a certain $d_i > 0$. As S is integral over R, for any i we have a relation of the form:

$$T_i^N + r_{N-1} T_i^{N-1} + ... + r_0 = 0 \qquad (2)$$

with $N > 0$ and $r_k \in R$ for $0 \leq k < N$.

Each r_k can be written as a polynomial a_k with coefficients in K on the elements $\{f_j, 1 \leq j \leq m\}$, i.e.,

$$r_k(T_1,..,T_n) = a_k(f_1(T_1,..,T_n),..,f_m(T_1,..,T_n))$$

In order to have the integral relation(2)verified , there must exist at least one r_k with a pure monomial term on T_i. Then there is at least one f_j which is a pure monomial on T_i, because if $f_j(0,..,0,T_i,0,..,0) = 0$ for $1 \leq j \leq m$, then $r_k(0,..,0,T_i,0,..,0) = a_k(0,..,0) \in K$, so r_k would not have a pure monomial term on T_i.

Let d_i be the minimal positive integer such that $T_i^{d_i} \in R$. Consider $\mathcal{F}_0$ a minimal monic monomial generating system of the ideal R_+. It contains all the monomials $T_i^{d_i}$ for $1 \leq i \leq n$.

Assume $\mathcal{F}_0$ contains another monomial of the form $\prod_{i=1}^n T_i^{b_i}$. Because of the minimality of $\mathcal{F}_0$ the exponents b_i verify that $0 \leq b_i < d_i, \forall 1 \leq i \leq n$ and because of the minimality of d_i there are at least two indices –that we can assume to be 1 and 2– such that $b_1, b_2 > 0$.

Let $\mathcal{B}$ be a monomial monic basis of S over R. Then $\mathcal{B}$ contains 1 and all the monomials of the form $T_i^{a_i}$ with $1 \leq a_i < d_i$ for $1 \leq i \leq n$. In particular $T_1^{d_1-b_1} \in \mathcal{B}$ and we have a relation $(\prod_{i=1}^n T_i^{b_i})T_1^{d_1-b_1} = T_1^{d_1}(\prod_{i=2}^n T_i^{b_i})$ where : $\prod_{i=1}^n T_i^{b_i} \in R$, $T_1^{d_1-b_1} \in \mathcal{B}$, $T_1^{d_1} \in R$, $\prod_{i=2}^n T_i^{b_i} \in S$

Writing $\prod_{i=2}^n T_i^{b_i}$ as a product of a monomial in R and a monomial in $\mathcal{B}$ not containing T_1, we would have a non trivial linear relation over R of two elements of the basis $\mathcal{B}$, and this is a contradiction. If follows that $R = K[T_1^{d_1},..,T_n^{d_n}]$ and R is a polynomial algebra since the elements $\{T_1^{d_1},..,T_n^{d_n}\}$ are algebraically independent over K.

□

We summarize the results of the last two sections as follows.

Theorem 4.2. *Let S be a polynomial algebra defined over K generated by the variables $\{T_1,..,T_m\}$ and graded in the natural way. Assume that there exist K-linear homogeneous operators $P, \Delta_1,..,\Delta_n : S \to S$ such that:*

(i) *The operators Δ_i are of degree -1, P is of degree 0 and $P(1) = 1$.*
(ii) *The operators Δ_i and P are S^Δ–linear, i.e., $\forall x \in S^\Delta, \forall y \in S$ we have $P(xy) = xP(y)$ and $\Delta_i(xy) = x\Delta_i(y)$. Here we abbreviate $\Delta = \{\Delta_1,..,\Delta_n\}$.*
(iii) *If $\mathcal{I} \subset S$ is a homogeneous ideal that for all $i = 1,2,..n$ is Δ_i-stable, then $\mathcal{I}$ is also P-stable and the sequence*

$$S/\mathcal{I} \xrightarrow{\widehat{P}} S/\mathcal{I} \xrightarrow{\widehat{\Delta_1}\oplus..\oplus\widehat{\Delta_n}} S/\mathcal{I} \oplus ... \oplus S/\mathcal{I}$$

is exact where $\widehat{P}, \widehat{\Delta_1},..,\widehat{\Delta_n}$ are the corresponding maps defined on the quotient.
(iv) *The K–space $S/S_+^\Delta S$ is finite dimensional.*

Then the subalgebra S^Δ is polynomial and in the case it can be generated over K by monomials it is of the form $K[T_1^{d_1},..,T_m^{d_m}]$ for certain positive integers d_i.

5. Examples of polynomial invariants

In this section we illustrate the results proved before with some examples. First we show that the theorem of Chevalley-Shephard-Todd can be proved using the methods developed above. Then we exhibit an example that is not covered by the classical results.

We start by reviewing some well known definitions and constructions.

Let K is an arbitrary field and $T : K^n \to K^n$ an invertible linear map. T is called a pseudo-reflection if $\dim_K \mathrm{Ker}(T - id) = n-1$. The structure of a pseudo-reflection can determined exactly. The condition about the rank guarantees that it has 1 as eigenvalue with multiplicity at least $n-1$. Two alternatives are possible: the other eigenvalue is different from one in which case the matrix will be diagonalizable to a matrix of the form $S_\alpha = \mathrm{diag}(1, 1, .., 1, \alpha)$; the other eigenvalue is one in which case the matrix cannot be diagonalizable, and is similar to a matrix of the form

$$S_\infty = \begin{pmatrix} 1 & 0 & 0 & ... & 0 & 0 & 0 \\ 0 & 1 & 0 & ... & 0 & 0 & 0 \\ 0 & 0 & 1 & ... & 0 & 0 & 0 \\ . & . & . & ... & . & . & . \\ . & . & . & ... & . & . & . \\ 0 & 0 & 0 & ... & 1 & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 & 1 \\ 0 & 0 & 0 & ... & 0 & 0 & 1 \end{pmatrix}$$

A diagonalizable pseudo-reflection will be called strong. The only strong pseudo-reflections are the ones of type S_α. A seudo-reflection T with finite order not divided by the characteristic of K is authomatically strong. The pseudo-reflections of type S_∞ are of finite order only if the base field has positive characteristic.

Let T be a strong seudo-reflection and call $f_T : K^n \to K$ a linear functional dual to $\mathrm{Ker}(T - id)$, a_T the T–eigenvalue different from 1 and v_T the a_T–eigenvector of T such that $f_T(v_T) = 1$. Then $T = id + (a_T - 1)f_T v_T$ and $T^{-1} = id + (a_T^{-1} - 1)f_T v_T$.

The action of T on K^n induces an action of T on $(K^n)^*$ by the formula $(T.f)(v) = f(T^{-1}v)$ or more explicitly $T.f = f + (a_T^{-1} - 1)f(v_T)f_T$. This action of T on $(K^n)^*$ can be extended by multiplicativity to the symmetric algebra $S = S((K^n)^*)$. The following result is well known and easy to prove.

Lemma 5.1. *In the situation above there exists a linear operator $\Delta_T : S \to S$ homogeneous of degree -1 such that: $\forall \xi \in S$, $T.\xi - \xi = f_T\Delta_T(\xi)$, $\Delta_T(\xi\eta) = \xi\Delta_T(\eta) + \eta\Delta_T(\xi) + f_T\Delta_T(\xi)\Delta_T(\eta)$.*

Let G be a finite linear group and consider its natural action on K^n. For any strong pseudo-re/-flec/-tion $s \in G$ we associate an operator Δ_s as above. In the case in which $\mathrm{char}(K)$ is prime with the order of G –and hence the pseudo-reflections are strong–we can also consider the standard projection P from S to S^G. Assume that $s_1, .., s_n$ is a list of all the pseudo-reflections of G and that we call $\Delta_1, .., \Delta_n$ the corresponding operators. If G is generated by $s_1, .., s_n$, the operators $P, \Delta_1, .., \Delta_n$ verify the hypothesis of Theorem 4.2.

First observe that $S^\Delta = \{\xi \in S : \Delta_i(\xi) = 0, i = 1,..,n\} = \{\xi \in S : s_i.\xi = \xi, i = 1,..,n\} = \{\xi \in S : g.\xi = \xi \ \forall g \in G\} = S^G$. It is clear that P is S^G-linear. If we apply the formula $\Delta_i(\xi\eta) = \xi\Delta_i(\eta) + \Delta_i(\xi)\eta + f_i\Delta_i(\xi)\Delta_i(\eta)$ for $\xi \in S, \eta \in S^G$ we conclude that the operators Δ_i are S^G–linear.

If $\mathcal{I}$ is a Δ_i–stable ideal, it is also stable by s_i for all $i = 1,..,m$ and hence it is G–stable. Finally if we have an element $\xi + \mathcal{I} : \Delta_i(\xi) \in \mathcal{I}$ for $i = 1,..,n$, then $s_i.\xi - \xi \in \mathcal{I}$ for all i. As the set $\{s_i : i = 1,..,n\}$ generate G, we conclude that $g.\xi - \xi \in \mathcal{I}, \ \forall g \in G$. Adding all the above relations we conclude that $P(\xi) - \xi \in \mathcal{I}$. Hence $\xi + \mathcal{I} \in \operatorname{Im}(\widehat{P})$ and the sequence:

$$S/\mathcal{I} \xrightarrow{\widehat{P}} S/\mathcal{I} \xrightarrow{\widehat{\Delta_1}\oplus..\oplus\widehat{\Delta_n}} S/\mathcal{I} \oplus ... \oplus S/\mathcal{I}$$

is exact.

The hypothesis about the finiteness of the dimension of S/S^G_+S as a K–space follows easily from the well known fact that in the case of a finite group the extension $S^G \subset S$ is integral.

Next example shows that the operators also appear in a completely different context than the classical case above.

Suppose that K is a field of characteristic 2, and consider the graded polynomial ring $S = K[X,Y]$. Consider δ_1, δ_2 the K-linear derivations of S defined over the generators by the formulae:

$$\begin{array}{ll} \delta_1(X) = Y & \delta_1(Y) = 0 \\ \delta_2(X) = Y & \delta_2(Y) = Y \end{array}$$

Call $K_n[X,Y]$ the homogeneous component of degree n of the original polynomial algebra. On the K–basis $\{X^n, X^{n-1}Y, .., XY^{n-1}, Y^n\}$ of $K_n[X,Y]$, the matrices associated to δ_1 and δ_2 –that we call D_1 and D_2– are the following:

$$D_1 = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & 0 & 0 \\ n & 0 & 0 & ... & 0 & 0 & 0 \\ 0 & n-1 & 0 & ... & 0 & 0 & 0 \\ 0 & 0 & n-2 & ... & 0 & 0 & 0 \\ . & . & . & ... & . & . & . \\ . & . & . & ... & . & . & . \\ 0 & 0 & 0 & ... & 2 & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 & 0 \end{pmatrix}$$

$$D_2 = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & 0 & 0 \\ n & 1 & 0 & ... & 0 & 0 & 0 \\ 0 & n-1 & 2 & ... & 0 & 0 & 0 \\ 0 & 0 & n-2 & ... & 0 & 0 & 0 \\ . & . & . & ... & . & . & . \\ . & . & . & ... & . & . & . \\ . & . & . & ... & 2 & n-1 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 & n \end{pmatrix}$$

As the matrices verify $D_2 = D_1 + \operatorname{diag}(0,1,..,n)$, $\operatorname{Ker}(D_1) \cap \operatorname{Ker}(D_2) = \operatorname{Ker}(D_1) \cap \operatorname{Ker}(\operatorname{diag}(0,1,..,n))$. Let $\{e_n, e_{n-1}, .., e_0\}$ be the canonical basis of K^{n+1}.

If n is even one easily checks that $\operatorname{Ker}(D_1) = \operatorname{Ker}(\operatorname{diag}(0,1,..,n)) = \langle e_n, e_{n-2}, .., e_0 \rangle$.

If n is odd of the form $n = 2k+1$, we have that $\mathrm{Ker}(D_1) = \langle e_{2k}, e_{2k-2}, .., e_0\rangle$ and
$\mathrm{Ker}(\mathrm{diag}(0,1,..,2k+1)) = \langle e_{2k+1}, e_{2k-1}, .., e_1\rangle$.

Hence the homogeneous n-th component of $\mathrm{Ker}(\delta_1) \cap \mathrm{Ker}(\delta_2)$ is:

$$\begin{array}{cc} 0 & if \quad n = 2k+1 \\ \langle X^{2k}, X^{2k-2}Y^2, .., X^2Y^{2k-2}, Y^{2k}\rangle & if \quad n = 2k \end{array}$$

We conclude that $\mathrm{Ker}(\delta_1) \cap \mathrm{Ker}(\delta_2) = K[X^2, Y^2]$.

The direct computation above, that implies that $\mathrm{Ker}(\delta_1)\cap\mathrm{Ker}(\delta_2)$ is a polynomial ring, can be explained in terms of the theory developed before.

Call Δ_1 and Δ_2 the differentiation operators of degree –1 in $K[X, Y]$ defined as:

$$\begin{array}{cc} \Delta_1(X) = 1 & \Delta_1(Y) = 0 \\ \Delta_2(X) = 1 & \Delta_2(Y) = 1 \end{array}$$

As $\delta_1 = Y\Delta_1$ and $\delta_2 = Y\Delta_2$, $\mathrm{Ker}(\Delta_1) \cap \mathrm{Ker}(\Delta_2) = \mathrm{Ker}(\delta_1) \cap \mathrm{Ker}(\delta_2)$.

Now we find the operator P of Theorem 4.2.

It is clear that any polynomial $f \in K[X, Y]$ can be decomposed in a unique form in the following way: $f(X, Y) = f_1(X^2, Y^2) + Xf_2(X^2, Y^2)+ +Yf_3(X^2, Y^2) + XYf_4(X^2, Y^2)$

We define the operator $P : K[X, Y] \to K[X, Y]$ by the formula : $P(f) = f_1$. In more explicit terms $P(\sum_{n,m} a_{n,m}X^nY^m) = \sum_{k,h} a_{2k,2h}X^{2k}Y^{2h}$.

Clearly P, Δ_1, Δ_2 are $K[X^2, Y^2]$–linear.

It follows that:

$\Delta_1(f) = f_2(X^2, Y^2) + Yf_4(X^2, Y^2)$

$\Delta_2(f) = f_2(X^2, Y^2) + f_3(X^2, Y^2) + (X + Y)f_4(X^2, Y^2)$.

From the above equalities we easily deduce that if an ideal $\mathcal{I}$ is stable by Δ_1 and Δ_2 then $f \in \mathcal{I}$ if and only if $f_1, f_2, f_3, f_4 \in \mathcal{I}$.

Now we check condition (iii) of Theorem 4.2.

Let $\mathcal{I}$ be a Δ_i–stable ideal of $K[X, Y]$ for $i = 1, 2$ and assume that $f \in K[X, Y]$ is such that $\Delta_1(f) \in \mathcal{I}$ and $\Delta_2(f) \in \mathcal{I}$. Hence : $f_2 + Yf_4 \in \mathcal{I}, f_2 + f_3 + (X + Y)f_4 \in \mathcal{I}$.

Applying Δ_2 to the first equality we conclude first that $f_4 \in \mathcal{I}$ and then that $f_2, f_3 \in \mathcal{I}$. Hence $f - f_1 \in \mathcal{I}$ and consequently the element f belongs to the image of P in the quotient $K[X, Y]/\mathcal{I}$.

It is interesting to observe that the above example is not covered by the classical theory of Chevalley, Shephard and Todd. Indeed it is not hard to prove that the subalgebra $K[X^2, Y^2]$ of $K[X, Y]$ is not realizable as the algebra of invariants of a finite group G acting linearly on K^2. In characteristic zero this can be proved using for example Poincaré series and in the characteristic 2 case a direct argument can be given.

References

[1] N. Bourbaki: *Éléments de mathématiques. Fasc. XXXIV. Groupes Groupes et Algèbres de Lie.* Chapitre V. Hermann, Paris.

[2] C. Chevalley: Invariants of finite groups generated by reflections. *American J. of Math.*, **77**, 778-782 (1955).

[3] F. Klein : *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom füntften Grade.* Teubner, 1884. Leipzig.

[4] H. Matsumura: *Commutative Algebra.* W. A. Benjamin Inc, 1970. New York.

[5] G. C. Shepard, J. A. Todd : Finite unitary reflection groups. *Canadian J. of Math .* **6**, 274-304 (1954).

[6] T. A. Springer : *Invariant Theory.* Lecture Notes in Mathematics **585**. Springer-Verlag. Berlin, Heidelberg, New York.

[7] H. Weyl : *The Classical Groups. Their Invariants and Representations.* Princeton University Press. 1939. New Jersey.

Walter Ferrer Santos

Centro de Matemática.Eduardo Acevedo 1139. C.P. 11.200. Montevideo.Uruguay.

wrferrer@cmat.edu.uy

Gerardo Gonzalez-Sprinberg

Inst.Fourier.Université Grenoble I. B.P.74.38402 Saint-Martin-d'Hères.France.

gonsprin@fourier.ujf-grenoble.fr