Illinois Journal of Mathematics
Volume 51, Number 1, Spring 2007, Pages 299–311
S 0019-2082

FIELD DEGREES AND MULTIPLICITIES FOR NON-INTEGRAL EXTENSIONS

BERND ULRICH AND CLARENCE W. WILKERSON

Dedicated to Phil Griffith, for his numerous contributions to algebra

Abstract. Let R be a graded subalgebra of a polynomial ring S over a field so that S is algebraic over R. The goal of this paper is to relate the generator degrees of R to the degree $[S:R]$ of the underlying quotient field extension, and to provide a numerical criterion for S to be integral over R that is based on this relationship. As an application we obtain a condition guaranteeing that a ring of invariants of a finite group is a polynomial ring.

1. Introduction

Let k be a field and $S = k[t_1, \dots, t_d]$ a polynomial ring with variables t_i of degree one. Consider a k-subalgebra R generated by m homogeneous elements $\{x_1, \dots, x_m\}$. In general, if x is a homogeneous element in a graded object, we denote its degree by $|x|$.

Problem. *If S is algebraic over R, calculate $[S:R]$ from the $\{|x_i|\}$.*

First, one has a form of Bezout's Theorem:

Theorem 1.1. *If S is integral over R, the following hold:*
(a) *$[S:R]$ divides $\prod |x_i|$.*
(b) *If $m = d$, then $[S:R] = \prod |x_i|$.*

In this paper we obtain a converse to part (b) above:

Theorem 1.2. *If S is algebraic over R, the following hold:*
(a) *$[S:R] \leq \prod |x_i|$.*

Received November 6, 2006; received in final form March 19, 2007.

2000 *Mathematics Subject Classification.* Primary 13A50, 13B21. Secondary 13A30, 13D40, 13H15.

Bernd Ulrich was supported by NSF grant DMS-0501011. Clarence Wilkerson was supported by an NSF FRG grant, DMS-0354787.

(b) *If $[S:R] \geq \prod |x_i|$, then S is integral over R (equivalently, S is finitely generated as an R-module) and $R = k[y_1, \ldots, y_d]$ is a polynomial ring with variables $\{y_1, \ldots, y_d\} \subset \{x_1, \ldots, x_m\}$.*

We also note that if S is not integral over R, then $[S:R]$ need not divide $\prod |x_i|$ even for $m = d$.

Our proofs rely on reduction to the case of standard graded k-algebras. By a *standard graded* k-algebra we mean a positively graded k-algebra that is Noetherian and generated by its homogeneous elements of degree one (equivalently, is generated by finitely many homogeneous elements of degree one). For such an algebra A the Hilbert function $H_A(n) = \dim_k A_n$ is eventually polynomial,

$$H_A(n) = e(A)\, n^{d-1}/(d-1)! + \text{lower order terms}\,.$$

Here d is the Krull dimension, $\dim A$, of A, whereas the positive integer $e(A)$ is defined to be the *multiplicity* of A. More generally, if M is a finitely generated graded A-module, one has

$$H_M(n) = e(M)\, n^{d-1}/(d-1)! + \text{ lower order terms}$$

for $n \gg 0$, where $d = \dim M$ is the Krull dimension of M as an A-module and $e(M)$ denotes its multiplicity; see, e.g., [4, 4.1.3].

We will deduce Theorem 1.2 from the next result that provides a criterion for integrality in terms of multiplicities:

Theorem 1.3. *Let $A \subset B$ be an inclusion of standard graded k-algebras which are domains and for which B is algebraic over A. One has:*

(a) $e(B) \geq [B:A]\; e(A)$.

(b) $e(B) = [B:A]\; e(A)$ *if and only if $A \subset B$ is integral.*

An interesting application of Theorem 1.2(b) is in the study of rings of invariants of finite groups acting on a polynomial ring:

Theorem 1.4. *Let V be a d-dimensional vector space over the field k, V^* its k-dual, and $S = k[V^*] = k[t_1, \ldots, t_d]$ the algebra of polynomial functions on V. Let $W \subset GL(V)$ be a finite group and consider the induced action on S. Then $R = S^W$ is a polynomial algebra over k if and only if there exist homogeneous elements $\{x_1, \ldots, x_d\}$ of R such that*

(a) *S is algebraic over $k[x_1, \ldots, x_d]$, and*

(b) $|W| \geq \prod |x_i|$.

Notice that we do not assume $\{x_1, \ldots, x_d\}$ to form a system of parameters of S, as was done in [14, 5.5.5].

In the last section, we give examples of rings of invariants for which Theorem 1.4 is useful in providing a proof of polynomial structure.

We note that Theorem 1.3 is a special case of results by Simis-Ulrich-Vasconcelos [13, 6.1]. However, the stronger hypotheses here make a streamlined proof possible. We have also included more details of the graded algebra computations in order to make the paper accessible to the wider audiences of invariant theorists and algebraic topologists.

2. Proof of Theorem 1.1

We borrow the proof from Adams-Wilkerson [2].

Proof of Theorem 1.1. First notice that $\dim R = d$, since S is integral over R and S is a polynomial ring in d variables. Pick a homogeneous generating set $\{s_i | 1 \leq i \leq M\}$ for the finitely generated graded R-module S. Choose a basis for the quotient field L of S over the quotient field K of R consisting of homogeneous elements $\{u_j | 1 \leq j \leq N\}$ from S. Here $N = [S : R]$. Let U be the graded R-submodule of S generated by the $\{u_j\}$. Then U is a free graded R-module. Note that for each i, there exist homogeneous elements $\{a_{ij}\}$ and $\{b_{ij}\}$ in R so that $b_{ij} \neq 0$ and $s_i = \sum (a_{ij}/b_{ij}) u_j$. Then, taking $\Delta = \prod_{i,j} b_{ij}$ one obtains $\Delta S \subset U \subset S$.

We now record some Hilbert-Poincaré series:

(a) $P_S(T) = (1 - T)^{-d}$.
(b) $P_{\Delta S}(T) = T^{|\Delta|} P_S(T)$.
(c) $P_U(T) = g(T) P_R(T)$, where g is a polynomial with non-negative integer coefficients and $g(1) = N = [S : R]$.
(d) $P_R(T) = h(T)(1 - T)^{m-d} \prod (1 - T^{|x_k|})^{-1}$, for h a polynomial with integer coefficients; indeed, the pole order of this rational function is at most $d = \dim R$ as can be seen from a graded Noether normalization of R.

From the inclusions

$$\Delta S \subset U \subset S$$

one sees that

$$P_{\Delta S}(T) \leq P_U(T) \leq P_S(T).$$

These inequalities should first be interpreted as holding for the non-negative integer coefficients of the powers of T in the respective formal power series. But each of the series also represents a real analytic function for T real and $|T| < 1$. In terms of these functions, we can restate the inequalities as

$$P_{\Delta S}(T) \leq P_U(T) \leq P_S(T) \ \text{ for } 0 \leq T < 1 \ .$$

After multiplying by $(1 - T)^d > 0$, one obtains

$$T^{|\Delta|} \leq g(T) h(T) \prod ((1 - T)/(1 - T^{|x_i|})) \leq 1 \ \text{ for } 0 \leq T < 1 \ .$$

These inequalities have meaning for the functions, although not necessarily for the series. Thus in the limit as $T \to 1$, one has

$$g(1)h(1)\prod |x_i|^{-1} = 1, \quad \text{or} \quad g(1)h(1) = |x_1| \cdot \ldots \cdot |x_m| \ .$$

Since $g(1) = N = [S : R]$, it follows that $[S : R]$ indeed divides $|x_1| \cdot \ldots \cdot |x_m|$. In the special case that $m = d$, R is a polynomial algebra and $h(T) = 1$. Thus (a) and (b) are both established. □

3. Reduction of the proof of Theorem 1.2 to Theorem 1.3

Step One: We first reduce to the case $m = d$. In fact, we may assume that the first d homogeneous generators $\{x_1, \ldots, x_d\}$ of R are algebraically independent over k. Set $R' = k[x_1, \ldots, x_d]$. Notice that $[S : R'] \geq [S : R]$ and $|x_1| \cdot \ldots \cdot |x_d| \leq |x_1| \cdot \ldots \cdot |x_m|$. Thus if (a) holds for $R' \subset S$, it also holds for $R \subset S$. Therefore we may replace R by R' in (a). Furthermore, the assumption of (b) for $R \subset S$ implies

$$[S : R'] \geq [S : R] \geq |x_1| \cdot \ldots \cdot |x_m| \geq |x_1| \cdot \ldots \cdot |x_d| \geq [S : R'] \, .$$

Thus the assumption of (b) is satisfied for $R' \subset S$, and $[S : R'] = [S : R]$. In particular R' and R have the same quotient field. Once we have shown that S is integral over R', then S is integral over R and R is an integral extension of the polynomial ring R'. As R' is integrally closed and R is contained in the quotient field of R', it follows that $R = R'$. Thus indeed S is integral over R, and $R = R'$ is a polynomial ring in the variables $\{x_1, \ldots, x_d\} \subset \{x_1, \ldots, x_m\}$. Therefore in part (b) too, we may replace R by R'.

Step Two: In $R = k[x_1, \ldots, x_d]$ consider the subalgebra $R' = k[x_1^{k_1}, \ldots, x_d^{k_d}]$, where the positive integers $\{k_i\}$ are chosen so that for every i, $|x_i^{k_i}| = N$, the least common multiple of the $|x_i|$. Furthermore let $S^{(N)}$ denote the *Veronese subring* of S generated by all homogeneous elements of S whose degree is an integer multiple of N. Notice that both extensions $R' \subset R$ and $S^{(N)} \subset S$ are integral.

Step Three: We have an inclusion $R' \subset S^{(N)}$ in which all elements of each algebra have degree a multiple of N. Regrade the algebras by declaring the new grading to be the old grading divided by N. Then $R' \subset S^{(N)}$ can be regarded as an inclusion of standard graded domains, so Theorem 1.3 applies:

$$e(S^{(N)}) \geq [S^{(N)} : R'] \ e(R')$$

and

$$e(S^{(N)}) = [S^{(N)} : R'] \ e(R')$$

if and only if $R' \subset S^{(N)}$ is integral.

We now need some small calculations.

LEMMA 3.1. $e(R') = 1$.

Proof. This follows since R' is a polynomial algebra on degree one generators. □

Lemma 3.2. $e(S^{(N)}) = N^{d-1}$.

Proof. Since $S^{(N)}$ is a Veronese subring, we have $H_{S^{(N)}}(n) = H_S(Nn)$. Therefore

$$e(S^{(N)})\, n^{d-1}/(d-1)! + \ \cdots \ = e(S)\,(Nn)^{d-1}/(d-1)! + \ \cdots$$

and we obtain $e(S^{(N)}) = N^{d-1}e(S) = N^{d-1}$. □

Lemma 3.3. *$[S : S^{(N)}] = N$.*

Proof. Notice that $\{t_1^i\,|\,0 \le i \le N-1\}$ is a vector space basis for the quotient field of S over that of $S^{(N)}$. □

Lemma 3.4. *If $m = d$, then $[R : R'] = \prod k_i$.*

Proof. This can be easily seen by considering a basis of R as an R'-module. □

Lemma 3.5. *If $m = d$, then $[S : R] \prod k_i = [S : R'] = [S^{(N)} : R']\ N$.*

Proof. One has the chains of inclusions $R' \subset R \subset S$ and $R' \subset S^{(N)} \subset S$, and likewise on the quotient field level. Now use Lemmas 3.3 and 3.4. □

Lemma 3.6. *Assume that $m = d$. Then*

$$\frac{[S : R]}{\prod |x_i|} = \frac{[S^{(N)} : R']\ e(R')}{e(S^{(N)})}\ .$$

Proof. Notice that $|x_i| = N/k_i$. Now divide both sides of the equality in Lemma 3.5 by N^d, and use Lemmas 3.1 and 3.2. □

Lemma 3.7. *S is integral over R if and only if $S^{(N)}$ is integral over R'.*

Proof. If S is integral over R, then S is integral over R', and hence $S^{(N)}$ is integral over R'. On the other hand, if $S^{(N)}$ is integral over R', then S is integral over R', and hence over R. □

To prove Theorem 1.2(a) we apply Theorem 1.3(a) to the inclusion $R' \subset S^{(N)}$ and use Lemma 3.6, which shows that the inequalities of Theorems 1.2(a) and 1.3(a) are equivalent. Similarly, Theorem 1.2(b) is a consequence of Theorem 1.3(b) and Lemmas 3.6 and 3.7.

4. Proof of Theorem 1.3

To prove Theorem 1.3 it will be convenient to consider the more general class of *quasi-standard graded* algebras over a field k. By this we mean positively graded k-algebras A so that A is Noetherian, $A_0 = k$, and A is integral over the k-subalgebra generated by the homogeneous elements of degree one. As such algebras are finitely generated graded modules over standard graded k-algebras, one can define the concepts of Hilbert functions and multiplicities as in the standard graded case.

In this section, $A \subset B$ is an inclusion of quasi-standard graded k-domains for which B is algebraic over A. The aim is to prove that under suitable restrictions on the multiplicities of A and B, the ring B must be a finitely generated A-module. More specifically, we have the following generalization of Theorem 1.3:

Theorem 4.1. *Let $A \subset B$ be an inclusion of quasi-standard graded k-algebras which are domains and for which B is algebraic over A. One has:*

(a) $e(B) \geq [B : A]\ e(A)$.
(b) $e(B) = [B : A]\ e(A)$ *if and only if $A \subset B$ is integral.*

Notice that B contains a rank $[B : A]$ graded free module over A. Now part (a) of Theorem 4.1 follows by comparing the two Hilbert functions. One direction of the implication in (b) is standard:

Proposition 4.2. *Let $A \subset B$ be an inclusion of quasi-standard graded k-algebras which are domains. If B is integral over A, then $e(B) = [B : A]\ e(A)$.*

This can be deduced from a more general fact:

Proposition 4.3. *Let A be a quasi-standard graded k-algebra which is a domain, with quotient field K. If M is a finitely generated graded A-module with $\dim M = \dim A$, then $e(M) = \dim_K(M \otimes_A K)\ e(A)$.*

The proof of Proposition 4.3 is an easy adaptation of [10, 14.8].

The rest of this section is devoted to proving the other implication in Theorem 4.1(b). We first show that we can reduce to the case where $e(A) = e(B)$ and A and B are standard graded.

Given $A \subset B$ algebraic, choose homogeneous elements $\{c_i \,|\, 1 \leq i \leq N\}$ in B that form a basis for the quotient field L of B over the quotient field K of A. For each such c_i, there exists a nonzero homogeneous $a_i \in A$ such that $b_i = a_i c_i$ is integral over A. Define A' to be the A-subalgebra of B generated by the $\{b_i\}$. Then A' is integral over A and $[A' : A] = [B : A]$. Notice that A' is still quasi-standard graded, but that it may fail to be standard graded even if A and B are—hence the need to consider the wider class of quasi-standard graded algebras.

Thus by Proposition 4.2, since $A \subset A'$ is an integral extension of quasi-standard graded k-algebras,

$$e(A') = [A' : A]\ e(A)\ .$$

Hence if $e(B) = [B : A]\ e(A)$, one has $e(A') = e(B)$. Therefore the proof of Theorem 4.1(b) can be reduced to showing the following proposition:

Proposition 4.4. *Let $A \subset B$ be an inclusion of quasi-standard graded k-algebras which are domains and for which B is algebraic over A. If $e(B) = e(A)$, then B is a finitely generated A-module.*

Finally, the reduction to the standard graded case follows from some easy facts:

Lemma 4.5. *Let A be a quasi-standard graded k-algebra. There exists a positive integer N so that for each positive integer r, the Veronese subring $A^{(rN)}$ is generated by the elements of A_{rN} as a k-algebra. That is, after regrading, $A^{(rN)}$ is a standard graded k-algebra.*

Proof. One can take N to be the maximal degree occurring in a homogeneous minimal generating set of A, considered as a finitely generated module over a standard graded k-subalgebra. □

Lemma 4.6. *Let $A \subset B$ be an inclusion of quasi-standard graded k-domains such that B is algebraic over A. Let N be a positive integer. If $e(B) = e(A)$, then $e(B^{(N)}) = e(A^{(N)})$.*

Proof. All algebras involved have the same Krull dimension according to [8, Theorem A, p. 286], for instance. Now the lemma follows by comparing Hilbert functions. □

Lemma 4.7. *Let $A \subset B$ be an inclusion of quasi-standard graded k-domains. Let N be a positive integer. Then B is integral over A if and only if $B^{(N)}$ is integral over $A^{(N)}$.*

In light of Lemmas 4.5, 4.6 and 4.7 it will suffice to prove Proposition 4.4 in the standard graded case.

As in [13] the idea of the proof then is to consider the graded A-module C defined by the short exact sequence

$$0 \to A \to B \to C \to 0\ .$$

The module C has no obvious finiteness properties as an A-module, but it does have a Hilbert function, namely

$$H_C(n) = H_B(n) - H_A(n)\ .$$

Since B is algebraic over A, the two algebras have the same Krull dimension, say d; see, for instance, [8, Theorem A, p. 286]. As furthermore $e(A) = e(B)$, it follows that the leading term of $H_C(n)$ occurs in degree $d - 2$ or less.

We need to associate more structure to C in order to utilize this information about $H_C(n)$. Let $I = A_1B$ be the homogeneous B-ideal generated by A_1, the homogeneous elements of A having degree 1. Let G be the graded algebra associated to the filtration of B by powers of I. That is,

$$G = \bigoplus_{i=0}^{\infty} I^i/I^{i+1} \ .$$

Then G is a positively graded Noetherian ring, although in general it is not a domain and G_0 is not a field. It has Krull dimension $d = \dim B$. In fact, one has:

Proposition 4.8. *The associated graded ring G is equidimensional of dimension d. That is, for each minimal prime ideal $\mathfrak{p} \subset G$, $\dim G/\mathfrak{p} = \dim G = d$.*

Proof. The ring G can also be thought of as the quotient of the domain $\mathcal{R} = B[It, t^{-1}]$ (the extended Rees algebra) with respect to the principal ideal generated by t^{-1}. The Krull dimension of $\mathcal{R}$ is $d+1$; see [8, Theorem A, p. 286] or [10, 15.7]. The minimal prime ideals of G correspond to the minimal prime ideals of the principal ideal in $\mathcal{R}$ generated by t^{-1}. Let $\mathfrak{q}$ be such a prime ideal in $\mathcal{R}$. By the Krull Principal Ideal Theorem (see, e.g., [10, 13.5]), the height of $\mathfrak{q}$ is 1. Since $\mathcal{R}$ is an affine domain, we have $\dim \mathcal{R}/\mathfrak{q} = \dim \mathcal{R} - \operatorname{ht} \mathfrak{q}$; see, e.g., [8, 13.4]. Therefore

$$\dim \mathcal{R}/\mathfrak{q} = \dim \mathcal{R} - \operatorname{ht} \mathfrak{q} = (d+1) - 1 = d \ .$$

Hence if $\mathfrak{p} \subset G$ is the corresponding minimal prime ideal in G, then $\dim G/\mathfrak{p} = \dim \mathcal{R}/\mathfrak{q} = d$. That is, G is equidimensional of dimension d. □

Proposition 4.9. *In addition to the assumptions of Proposition* 4.4 *suppose that A and B are standard graded. Then the homogeneous ideal $B_1G \subset G$ is nilpotent.*

Proof of Proposition 4.4 using Proposition 4.9. In light of Lemmas 4.5, 4.6 and 4.7 we may assume that A and B are standard graded. Since B_1G is nilpotent according to Proposition 4.9, its filtration degree 0 component, B_1B/A_1B, is also nilpotent in G. Hence, back in B, $B_1B \subset \sqrt{A_1B}$. So there exists a positive integer N such that $B_1^N \subset A_1B_{N-1}$. As B is standard graded we deduce that $B_1^N = A_1B_1^{N-1}$ and then $B_n = A_{n-N+1}B_{N-1}$ for every $n \geq N$. Thus a generating set for B as an A-module can be obtained from a k-basis of $\bigoplus_{i=0}^{N-1} B_i$. That is, B is a finitely generated A-module. □

Proof of Proposition 4.9. The algebra G inherits an internal degree from B and a filtration degree from the I-adic filtration. We write $G_{(m,i)}$, where m is the internal degree and i is the filtration degree. For the total degree, we use the sum of the two degrees and set $G_n = \bigoplus_{m+i=n} G_{(m,i)}$. Note that since A and B are standard graded, $A_1^n = A_n$ and $B_1 B_{n-1} = B_n$ for every positive n. Thus

$$G_n = B_n/A_1B_{n-1} \oplus A_1B_{n-1}/A_2B_{n-2} \oplus \;\cdots\; \oplus A_{n-1}B_1/A_n \oplus A_n \ ,$$

and

$$(B_1G)_n = B_n/A_1B_{n-1} \oplus A_1B_{n-1}/A_2B_{n-2} \oplus \;\cdots\; \oplus A_{n-1}B_1/A_n \ .$$

This last expression gives us the “raison d'être” for G and B_1G in our strategy. When we take lengths, consecutive terms cancel. That is, $\dim_k (B_1G)_n = \dim_k B_n/A_n = \dim_k C_n$. Thus $H_{B_1G}(n) = H_C(n)$. Notice that with respect to the total degree, G is a standard graded (finitely generated) k-algebra and B_1G is a homogeneous G-ideal. Hence the Hilbert function and polynomial for B_1G detect the Krull dimension of B_1G as a module over G:

Lemma 4.10. $\dim B_1G \leq d-1$.

Proof. For $n \gg 0$, $H_{B_1G}(n) = H_C(n) = H_B(n) - H_A(n)$ is a polynomial function of degree $\leq d-2$, from the hypothesis that $e(A) = e(B)$. Since B_1G is a finitely generated graded module over the standard graded k-algebra G, its Krull dimension equals the degree of the Hilbert polynomial plus one; see, e.g., [4, 4.1.3]. □

On the other hand, one has $\dim B_1G = \dim G/\mathrm{ann}(B_1G)$, for $\mathrm{ann}(B_1G)$ the annihilator ideal of B_1G in G.

Lemma 4.11. *Let $\mathfrak{p} \subset G$ be a minimal prime ideal of G. Then $B_1G \subset \mathfrak{p}$.*

Proof. Proposition 4.8 shows that $\dim G/\mathfrak{p} = \dim G = d$ for every such $\mathfrak{p}$. On the other hand, $\dim G/\mathrm{ann}(B_1G) = \dim B_1G \leq d-1$ according to Lemma 4.10. Hence $\dim G/\mathrm{ann}(B_1G) < \dim G/\mathfrak{p}$, which implies that $\mathrm{ann}(B_1G) \not\subset \mathfrak{p}$. Since $\mathrm{ann}(B_1G) \cdot B_1G = 0 \subset \mathfrak{p}$ and $\mathfrak{p}$ is prime, it follows that $B_1G \subset \mathfrak{p}$. □

Now Lemma 4.11 immediately gives Proposition 4.9, because the nilradical of G is the intersection of its minimal prime ideals. □

5. Proof of Theorem 1.4 and a counterexample

We begin by recording a proof of Theorem 1.4.

Proof of Theorem 1.4. The forward implication is a consequence of Theorem 1.1(b). To show the converse, write $R' = k[x_1, \ldots, x_d]$ and notice that

$$[S : R'] \geq [S : R] = |W| \geq |x_1| \cdot \ldots \cdot |x_d| \ .$$

Applying Theorem 1.2 to the extension $R' \subset S$ we conclude that S is integral over R' (by part (b)) and that $[S : R'] = [S : R]$ (by part (a)). Thus R is integral over R' and the two rings have the same quotient field. But R' is a polynomial ring and hence integrally closed. It follows that $R' = R$. □

We finish this section with an example related to Theorem 1.2(a). It shows that the degree of the field extension need not divide the product of the degrees of the algebra generators.

Example 5.1. Let $S = k[x, y]$, where $|x| = |y| = 1$. Let R be the k-subalgebra of S generated by the monomials x^3 and xy^2. Let K be the quotient field of R and K' the extension given by adjoining the element x. Then $[K' : K] = 3$ and K' contains y^2. Hence the quotient field L of S is obtained from K' by adjoining y. Thus $[L : K'] = 2$, and $[L : K] = 6$, which does not divide $3^2 = 9$. There are of course no examples involving only one variable.

6. Applications to rings of invariants

A problem of interest in topology and invariant theory for the last thirty-five years has been the determination of which representations of finite groups have polynomial algebras as rings of invariants. Work of Shephard-Todd [11], Chevalley [5], Serre [12], Clark-Ewing [6], and others largely solved this problem in the case that the order of the group is a unit in the ground field. The work of Adams-Wilkerson [1] emphasized the connection of the problem to topology, even in the case where this condition fails.

Wilkerson, in [15, Section III], observed that often polynomial rings of invariants can be verified using this general strategy:

(a) pick d homogeneous elements $\{x_1, \ldots, x_d\}$ of S^W,
(b) verify that S is integral over R', the subalgebra generated by the $\{x_i\}$, and
(c) check that $[S : R'] = |W|$.

According to Theorem 1.1(b), for instance, in the presence of (b) item (c) is equivalent to

(c') check that $\prod |x_i| = |W|$.

He lists several types of finite linear groups in characteristic p for which this strategy works, for example, general linear groups (Dickson invariants), special linear groups and variations on the upper triangular groups. In these cases the integrality condition above is evident from the description of the invariants. Theorem 1.4 tells us that the integrality condition can be replaced by the weaker statement that the $\{x_i\}$ are algebraically independent.

Thus, computationally, given a choice of elements $\{x_i\}$ satisfying the above conditions (a) and (c'), one has two options:

(a) show that $\dim_k(S/I) < \infty$, for I the S-ideal generated by the $\{x_i\}$, or

(b) show that the Jacobian $|\partial x_i/\partial t_j|$, $1 \leq i, j \leq d$, is nonzero.

Computer algebra programs typically implement option (a) using Gröbner basis algorithms, and the time and memory requirements increase dramatically with the dimension d and the complexity of W. On the other hand, the Jacobian can be computed at points in $V \otimes_k \bar{k}$ by a combination of symbolic and numerical techniques that may be less demanding computationally.

In 1994, C. Xu [16], [17] studied three examples from the [11], [6] list of complex and p-adic reflection groups. These groups are labeled as W_{29}, W_{31} and W_{34} in characteristic 5, 5 and 7, and dimensions 4, 4, and 6 respectively. In each case he obtained a collection of invariant polynomial forms that allow Theorem 1.4 to be applied:

Theorem 6.1.

(a) *For the group W_{29} over $\mathbb{F}_5$, there are forty linear forms $\{L_i\}$ in $\mathbb{F}_5[t_1, \ldots, t_4]$ for which W_{29} permutes the powers $\{L_i^4\}$. The first, second, third, and fifth elementary symmetric polynomials$\{x_4, x_8, x_{12}, x_{20}\}$ in the $\{L_i^4\}$ are algebraically independent over $\mathbb{F}_5$ and the product of the degrees is $4 \cdot 8 \cdot 12 \cdot 20 = 7680 = |W_{29}|$.*

(b) *For the group W_{31} over $\mathbb{F}_5$, there is a degree 4 polynomial Y_4 in $\mathbb{F}_5[t_1, \ldots, t_4]$ for which the W_{31}-orbit contains only six distinct polynomials, $\{Y_{4,i}\}$. The second, third, fifth, and sixth elementary symmetric polynomials $\{y_8, y_{12}, y_{20}, y_{24}\}$ in the $\{Y_{4,i}\}$ are algebraically independent. The product of the degrees is $8 \cdot 12 \cdot 20 \cdot 24 = 46080 = |W_{31}|$.*

(c) *For the group W_{34} over $\mathbb{F}_7$, there are 126 linear forms $\{L_i\}$ in $\mathbb{F}_7[t_1, \ldots, t_6]$ for which the sixth powers $\{L_i^6\}$ are permuted by the action. The first, second, third, fourth, fifth, and seventh elementary symmetric polynomials $\{z_6, z_{12}, z_{18}, z_{24}, z_{30}, z_{42}\}$ in the $\{L_i^6\}$ are algebraically independent and the product of the degrees is $6 \cdot 12 \cdot 18 \cdot 24 \cdot 30 \cdot 42 = 39191040 = |W_{34}|$.*

The example W_{34} appears in his thesis [17] only, so we review the strategy briefly here. We begin with a method for finding some invariants. This works well for both W_{29} and W_{34}.

Let W be a subgroup of $GL(V)$, where V is a finite dimensional vector space over $k = \mathbb{F}_p$. Let $\mathcal{S}$ be the set of all reflections in W of order prime to p. These reflections are diagonalizable over k. Denote a typical such reflection by s. Let H_s denote the fixed hyperplane of s and f_s a linear form on V defining H_s.

Lemma 6.2. *For each $w \in W$, wH_s is fixed by wsw^{-1}. That is $wH_s = H_{wsw^{-1}}$.*

Proof. Let $v \in H_s$ and $w \in W$. Then $wsw^{-1}(wv) = ws(v) = wv$. □

Lemma 6.3. *W acts on the set of all H_s, for $s \in \mathcal{S}$.*

Now if f is a linear form on V to k, i.e., $f \in V^*$, define the action of W on V^* by $(wf)(v) = f(w^{-1}v)$, for $v \in V$.

Lemma 6.4. *Let $s \in \mathcal{S}$ and $w \in W$. Then $wf_s = \theta_{s,w} f_{wsw^{-1}}$, where $\theta_{s,w} \neq 0$ is an element of k. That is, up to units, the action of W permutes the linear forms defining the H_s.*

Proof. By Lemma 6.2, wf_s is zero on the hyperplane $wH_s = H_{wsw^{-1}}$. □

Proposition 6.5. *For V and W as above, the polynomials ${f_s}^{p-1}$ are permuted by the action of W.*

Proof. The multiplicative order of each $\theta_{s,w}$ is a divisor of $p - 1$. □

The group W_{34} has only one conjugacy class of reflections. This class has 126 elements and each has order 2. Thus the preceding theory can be applied to the sixth powers of the linear forms representing the hyperplanes for these reflections.

Xu was able to use the Gröbner basis routines of Macaulay to verify the specified generators for W_{29} and W_{31} (and, unstated, that S is integral over R'). In 1994, however, this failed for W_{34}. He therefore resorted to the Jacobian method. The Jacobian is not expanded as a degree 126 polynomial. Rather, each entry is evaluated at a point of the vector space and the resulting 6×6 determinant computed. In fact, it vanishes at each point of $(\mathbb{F}_7)^6$. However, Xu finds a point in $(\mathbb{F}_{49})^6$ where it is not zero. Thus the proposed generators are algebraically independent and by Theorem 1.4 the rings of invariants are as claimed by Xu:

Corollary 6.6.
(a) $\mathbb{F}_5[t_1, \ldots, t_4]^{W_{29}} = \mathbb{F}_5[x_4, x_8, x_{12}, x_{20}]$.
(b) $\mathbb{F}_5[t_1, \ldots, t_4]^{W_{31}} = \mathbb{F}_5[y_8, y_{12}, y_{20}, y_{24}]$.
(c) $\mathbb{F}_7[t_1, \ldots, t_6]^{W_{34}} = \mathbb{F}_7[z_6, z_{12}, z_{18}, z_{24}, z_{30}, z_{42}]$.
Here the degree of x_k, y_k, or z_k is k.

These examples can also be found in Aguadé [3], without proof of the polynomial nature of the rings of invariants. They are also included in [9].

References

[1] J. F. Adams and C. W. Wilkerson, *Finite H-spaces and algebras over the Steenrod algebra*, Ann. of Math. (2) **111** (1980), 95–143. MR 558398 (81h:55006)

[2] ———, *A correction: "Finite H-spaces and algebras over the Steenrod algebra"*, Ann. of Math. (2) **113** (1981), 621–622. MR 621021 (82i:55010)

[3] J. Aguadé, *Constructing modular classifying spaces*, Israel J. Math. **66** (1989), 23–40. MR 1017153 (90m:55016)

[4] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1993. MR 1251956 (95h:13020)

[5] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782. MR 0072877 (17,345d)

[6] A. Clark and J. Ewing, *The realization of polynomial algebras as cohomology rings*, Pacific J. Math. **50** (1974), 425–434. MR 0367979 (51 #4221)

[7] W. G. Dwyer and C. W. Wilkerson, *The elementary geometric structure of compact Lie groups*, Bull. London Math. Soc. **30** (1998), 337–364. MR 1620888 (99g:22007)

[8] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. MR 1322960 (97a:13001)

[9] G. Kemper and G. Malle, *The finite irreducible linear groups with polynomial ring of invariants*, Transform. Groups **2** (1997), 57–89. MR 1439246 (98a:13012)

[10] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986. MR 879273 (88h:13001)

[11] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304. MR 0059914 (15,600b)

[12] J.-P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, Colloque d'Algèbre (Paris, 1967), Exp. 8, Secrétariat mathématique, Paris, 1968, 11 pp. MR 0234953 (38 #3267)

[13] A. Simis, B. Ulrich, and W. V. Vasconcelos, *Codimension, multiplicity and integral extensions*, Math. Proc. Cambridge Philos. Soc. **130** (2001), 237–257. MR 1806775 (2002c:13017)

[14] L. Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995. MR 1328644 (96f:13008)

[15] C. Wilkerson, *A primer on the Dickson invariants*, Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982), Contemp. Math., vol. 19, Amer. Math. Soc., Providence, RI, 1983, pp. 421–434. MR 711066 (85c:55017)

[16] C. Xu, *Computing invariant polynomials of p-adic reflection groups*, Mathematics of Computation 1943–1993: a half-century of computational mathematics (Vancouver, BC, 1993), Proc. Sympos. Appl. Math., vol. 48, Amer. Math. Soc., Providence, RI, 1994, pp. 599–602. MR 1314898

[17] C. Xu, *The existence and uniqueness of simply connected p-compact groups with Weyl groups W such that the order of W is not divisible by the square of p*, Thesis, Purdue University, 1994.

Bernd Ulrich, Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA

E-mail address: `ulrich@math.purdue.edu`

Clarence W. Wilkerson, Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA

E-mail address: `cwilkers@purdue.edu`