FIELD DEGREES AND MULTIPlicITIES FOR NON-INTEGRAL EXTENSIONS

BERND ULRICH AND CLARENCE W. WILKERSON

1. INTRODUCTION

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

**Problem.** Let \([S : R]\) denote the degree of the underlying fraction field extension. 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 consider the case that \( m = d \) and obtain a converse to part (b) above:

**Theorem 1.2.** If \( S \) is algebraic over \( R \), \( m = d \), and \([S : R] = \prod |x_i|\), then \( S \) is integral over \( R \) (equivalently, \( S \) is finitely generated as an \( R \)-module).

We also note that if \( S \) is not integral over \( R \), then \([S : R]\) need not even divide \( \prod |x_i| \).

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:

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

*Date: *July 24, 2006.
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. [3, 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. One has

1. \(e(B) \geq [B, A] e(A)\).
2. \(e(B) = [B : A] e(A)\) if and only if \(A \subset B\) is integral.

An interesting application of Theorem 1.2 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 \(S = S[V^\#] = k[t_1, \ldots, t_d]\) the algebra of polynomial functions on \(V\). Let \(W \subset GL(V)\) be a finite group. There is an induced action on \(S\). Then \(S^W = R\) is a polynomial algebra over \(k\) if and only if there exist homogeneous elements \(\{x_1, \ldots, x_d\}\) of \(R\) such that

1. \(S\) is algebraic over \(k[x_1, \ldots, x_d]\), and
2. \(|W| = \prod |x_i|\).

In the last section, we give examples where \([B : A]\) does not divide \(\prod |x_i|\) and 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 [9, 6.1(b)]. 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 [1].

**Proof of 1.1:** Pick a homogeneous spanning set \(\{y_j\}_{j=1}^M\) for the finitely generated graded \(R\)-module \(S\). Choose a basis for the fraction field \(L\) of \(S\) over the fraction field \(K\) of \(R\) consisting of homogeneous elements \(\{u_i\}_{i=1}^N\) from \(S\). Here \(N = [S : R]\). Let \(U\) be the graded \(R\)-submodule of \(S\) generated by the \(\{u_i\}\). Then \(U\) is a free graded
Field Degrees

Note that for each $j$, there exist $\{a_{ij}\}$ and $\{b_{ij}\}$ in $R$ so that $b_{ij} \neq 0$ and $y_j = \sum (a_{ij}/b_{ij})u_j$. Then by taking $\Delta = \prod_{i,j} b_{ij}$, one has that $\Delta S \subset U \subset S$.

We now record some Hilbert-Poincaré series:

(a) $P_S(T) = (1 - T)^{-d}$.

(b) $P_R(T) = h(T)(1 - T)^{-m-d} \prod (1 - T^{\lvert x_i \rvert})^{-1}$, for $h$ a polynomial with integer coefficients.

(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) $P_{\Delta S}(T) = T^{|\Delta|}P_S(T)$.

From the inclusions

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

one has

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

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 $\lvert T \rvert < 1$. These functions each have a pole of order $d$ for $T = 1$. So in terms of these functions, we can restate the inequalities as

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

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

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

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

$$h(1)g(1) \prod \lvert x_i \rvert^{-1} = 1, \quad \text{or } h(1)g(1) = \lvert x_1 \rvert \cdots \lvert x_m \rvert.$$

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

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

**Step One:** Starting with $k[x_1, \ldots, x_d] = R$, obtain the subalgebra $R' = k[x_1^{k_1}, \ldots, x_d^{k_d}]$, where the positive integers $\{k_i\}$ are chosen so that for all $i$, $\lvert x_i^{k_i} \rvert = N$, the least common multiple of the $\lvert x_i \rvert$. Then $R' \subset R$ is integral.
Step Two: Replace $S$ by the Veronese subring $S^{(N)}$ generated by all homogeneous elements of $S$ whose degree is an integral multiple of $N$.

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 finitely generated standard graded domains, so Theorem 1.3 applies:

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

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. \hfill \Box

**Lemma 3.2.** $[S : S^{(N)}] = N$.

*Proof.* Notice that $\{(t_i)^i | 1 \leq i \leq N - 1\}$ is a vector space basis for the fraction field of $S$ over that of $S^{(N)}$. \hfill \Box

**Lemma 3.3.** $[R : R'] = \prod k_i$.

*Proof.* This can be easily seen by considering a basis of $R$ as an $R'$-module. \hfill \Box

**Lemma 3.4.** $[S : R] \prod k_i = [S : R'] = [S^{(N)} : R'] N$.

*Proof.* One has the chains of inclusions $R' \subset R \subset S$ and $R' \subset S^{(N)} \subset S$, and likewise on the fraction field level. Now use Lemmas 3.2 and 3.3. \hfill \Box

**Lemma 3.5.** $e(S^{(N)}) = N^{d-1}$. 

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

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

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

**Lemma 3.6.**

$$[S : R] = \prod |x_i|$$

if and only if

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

\[ [S : R] = \prod |x_i| \]
\[ \iff [S : R] \prod k_i = \prod (|x_i| k_i) \]
\[ \iff [S^{(N)} : R']^N = N^d \]
\[ \iff [S^{(N)} : R'] = N^{d-1} \]
\[ \iff e(S^{(N)}) = [S^{(N)} : R'] e(R') . \]

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 $R$.

Theorem 1.2 now follows from Theorem 1.3(b), Lemma 3.6 and Lemma 3.7.

4. Proof of Theorem 1.3

To prove Theorem 1.3 it will be more convenient to consider the more general class of quasi-standard graded $k$-algebras. 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.

Part (a) is clear since $B$ contains a rank $[B : A]$ free graded module over $A$. One direction of the implications 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 field of fractions $K$. If $M$ is a finitely generated graded $A$-module with $\dim M = \dim A$, then $e(M) = \dim_K(M \otimes_A K) e(A)$.

See [7, 14.8] for a proof of Proposition 4.3. The rest of this section is devoted to a proof of the other implication in 4.1(b).

We first prove that we can reduce to the case that $e(A) = e(B)$, $[B : A] = 1$, and $A$ and $B$ are standard graded.

Given $A \subset B$ algebraic, choose homogeneous elements $\{c_i \mid 1 \leq i \leq N\}$ in $B$ that form a basis for the field of fractions $L$ of $B$ over the field of fractions $K$ 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 the extension degree $[A' : A] = [B : A]$. Therefore $[B : A'] = 1$. 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,


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

Proposition 4.4. Let $A \subset B$ be an inclusion of quasi-standard graded $k$-domains such that $B$ is algebraic over $A$ and $e(B) = e(A)$. 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 algebra $A^{(rN)}$ is generated by the elements of $A_{rN}$. That is, after regrading, $A^{(rN)}$ is a standard graded $k$-algebra.

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 $[B^{(N)} : A^{(N)}] = 1$. 
Lemma 4.7. Let $A \subset B$ be an inclusion of quasi-standard graded $k$-domains. Choose a positive integer $N$. Then $B$ is integral over $A$ if and only if for the Veronese algebras, $B^{(N)}$ 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.

The idea of the proof then is to consider the graded $A$-module $C$ defined by the short exact sequence

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

$C$ 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 [6, 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 $A_1$. Let $G$ be the associated graded algebra 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 that of $B$, see e.g. [7, 15.7].

Proposition 4.8. The ring $G$ is equidimensional. That is, for each minimal prime ideal $p \subset G$, $\dim G/p = \dim G = d$.

Proof. The associated graded 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 [6, Theorem A, p. 286] or [7, 15.7]. The minimal prime ideals of $G$ correspond to the minimal prime ideals in $\mathcal{R}$ associated to the principal ideal generated by $t^{-1}$. Let $q$ be such an associated prime ideal in $\mathcal{R}$. By the Krull Principal Ideal Theorem, see e.g. [7, 13.5], the height of $q$ is 1. Since $\mathcal{R}$ is an affine domain, we have $\dim \mathcal{R}/q = \dim \mathcal{R} - \text{ht } q$, see e.g. [6, 13.4]. Therefore

$$\dim \mathcal{R}/q = \dim \mathcal{R} - \text{ht } q = (d + 1) - 1 = d.$$
Hence if $p \subset G$ is the corresponding minimal prime ideal in $G$, then $\dim G/p = \dim R/q = d$. That is, $G$ is equidimensional. \hfill \Box

**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 4.6 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 $B_N = A_1B_{N-1}$. As $B$ is standard graded we deduce that $B_N = A_1B_{N-1}$, and then $B_n = A_{n-N}B_N$ 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:**

$G$ inherits an internal degree from $B$ and a filtration degree from the $I$-adic filtration. We write $G_{(n,i)}$ where $n$ is the internal degree and $i$ is the filtration degree. For the total degree, we use the sum of the two degrees and set $G_m = \bigoplus_{n+i=m} G_{(n,i)}$. Note that since $A$ and $B$ are standard graded, $A_1A_{n-1} = A_n$ and $B_1B_{n-1} = B_n$ for all $n$. Thus

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

and

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

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 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 dimension is detected by the degree of the Hilbert polynomial, see e.g. [3, 4.1.3]. \hfill \Box
On the other hand, for \( \text{ann}(B_1G) \) the annihilator ideal of \( B_1G \) in \( G \), \( \dim B_1G = \dim G/\text{ann}(B_1G) \).

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

**Proof.** Since \( G \) is equidimensional, \( \dim G/\mathfrak{p} = \dim G = d \) for each such \( \mathfrak{p} \). Hence \( \text{ann}(B_1G) \not\subset \mathfrak{p} \) since \( \dim G/\text{ann}(B_1G) \leq d - 1 < \dim G/\mathfrak{p} \). Thus \( \text{ann}(B_1G) \) contains an element not in \( \mathfrak{p} \), i.e., in \( G - \mathfrak{p} \), so the localization \( (B_1G)_\mathfrak{p} = 0 \). Therefore \( B_1G \subset \mathfrak{p} \), since if \( B_1G \) contained an element not in \( \mathfrak{p} \), it would yield a unit in \( (B_1G)_\mathfrak{p} \). \( \square \)

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

## 5. Counterexamples and examples

We first construct an example for \( d = 2 \) for which the field extension degree does 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 \( x^2 \) and \( xy^2 \). Let \( K \) be the fraction field of \( R \) and \( K' \) the extension given by adjoining the element \( x \). Then \( [K' : K] = 3 \) and \( K' \) contains \( y^2 \). Hence the fraction 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.

The second class of examples are illustrations of Theorem 1.4. Wilkerson [10, Section III] lists several types of finite linear groups in characteristic \( p \) for which one obtains polynomial rings of invariants. In addition to the Dickson invariants for the general linear groups, the special linear groups and variations on the upper triangular groups qualify. But in these cases, the integrality conclusion of Theorem 1.4 is already evident.

However, the Shephard-Todd [8] list of finite complex reflection groups provides more challenges. Clark-Ewing [4] analyze these to determine for each group the primes for which there is an associated reflection representation over the \( p \)-adic integers or \( \mathbb{F}_p \). C. Xu in [11, 12] studied the three complex reflection groups labeled \( W_{29} \), \( W_{31} \) and \( W_{34} \) in characteristic 5, 5 and 7, respectively. In each case he obtained a list of invariant polynomial forms that allow Theorem 1.4 to be applied:
Theorem 5.2.

(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 $W_{31}$ 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 $6 \cdot 12 \cdot 18 \cdot 24 \cdot 30 \cdot 42 = 39191040 = |W_{34}|$.

For $W_{29}$ and $W_{31}$, Xu uses the computer algebra program Macaulay to verify that the proposed generators are algebraically independent. However, for example $W_{34}$, the number and degree of the terms involved force a different strategy. The Jacobian is set up but not expanded symbolically. In fact, it vanishes at each point of $(\mathbb{F}_7)^6$. However, Xu finds a point in $(\mathbb{F}_{49})^6$ for which this Jacobian does not vanish. That is, the Jacobian is not identically zero, so the the proposed generators are algebraically independent. Thus, by Theorem 1.4, the rings of invariants are as claimed by Xu:

Corollary 5.3.

(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) $\mathbb{F}_7[t_1, \ldots, t_6]^{W_{34}} = \mathbb{F}_5[z_6, z_{12}, z_{18}, z_{24}, z_{30}, z_{42}]$.

Here the degree of $x_k$, $y_k$, or $z_k$ is $k$.

These examples can also be found in Aguadé [2] without proof of the polynomial nature of the rings of invariants.
References


Department of Mathematics, Purdue University, West Lafayette, IN 47907

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