On Vector Invariants over Finite Fields

DAVID R. RICHMAN

Department of Mathematics, University of South Carolina, Columbia, South Carolina 29208

Let $F$ denote a finite field and let $S(m, n, F)$ denote a set of generators of the invariants of $\text{SL}(n, F)$ acting on $m$ $n$-component vectors. This paper proves that if $m > n > 1$, then $S(m, n, F)$ must contain a generator whose degree is greater than or equal to $(m - n + 2)(|F| - 1)$. Similar results are obtained for the vector invariants of other groups of matrices with entries in $F$. © 1990 Academic Press, Inc.

0. INTRODUCTION

Let $K$ denote a field and let $U_1, ..., U_m, V_1, ..., V_m$ denote commuting indeterminates. If $x \in K$ and $f \in K(U_i, V_j : 1 \leq i \leq m)$, let $\sigma(x)$ denote the $K$-algebra automorphism of $K(U_i, V_j : 1 \leq i \leq m)$ which maps $U_i$ to $U_i$ and $V_i$ to $xU_i + V_i$ for every $i$ and let $f^{\sigma(x)}$ denote the image of $f$ under this automorphism. If $A \subseteq K$, let $\text{UT}(A) = \{ \sigma(x) : x \in A \}$; the letters UT in UT$(A)$ stand for “unipotent triangular,” coming from the matrix equation

\[
(U_i^{\sigma(x)}V_j^{\sigma(x)}) = (U_iV_j)^\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.
\]

Suppose that $A \subseteq K$ and $R \subseteq K(U_i, V_j : 1 \leq i \leq m)$. Let $R^{\text{UT}(A)}$ denote the set of elements of $R$ which are fixed by every automorphism in UT$(A)$; such elements are said to be invariants of UT$(A)$. Most of this paper is concerned with properties of sets of $K$-algebra generators of $K[U_i, V_j : 1 \leq i \leq m]^{\text{UT}(A)}$. Note that $\sigma(x) \circ \sigma(y) = \sigma(x + y)$ for all $x, y \in K$. Therefore, if $A'$ denotes the additive group generated by $A$, then $R^{\text{UT}(A)} = R^{\text{UT}(A')}$.

Hence, when studying the ring $R^{\text{UT}(A)}$, one may assume without loss of generality that $A$ is an additive subgroup of $K$.

It is known that

if $K$ is an infinite field, then

\[
K[U_i, V_j : 1 \leq i \leq m]^{\text{UT}(K)} = K[U_i, U_jV_j - U_jV_i : 1 \leq i, j \leq m].
\]

A proof of this result, in the case that $K$ is a field of characteristic zero, can be found in [18, pp. 47–49] and a proof in the general case can be found.
in [14, Proposition 7(i), p. 54] (in [14] the group $\text{UT}(K)$ is denoted $\text{UUT}(2, K)$). Suppose that $f \in K[U_i, V_i : 1 \leq i \leq m]$ and note that $f^{(x)}$ can be expressed as a polynomial in $x$ with coefficients in $K[U_i, V_i : 1 \leq i \leq m]$. Therefore, if $f^{(x)} - f = 0$ for more than $\deg f$ values of $x$, then $f^{(x)} - f = 0$ for all $x \in K$. This observation and statement (0.1) imply that

if $A$ is an infinite subset of $K$, then

$$K[U_i, V_i : 1 \leq i \leq m]^\text{UT(A)} = K[U_i, U_i V_j - U_j V_i : 1 \leq i, j \leq m].$$

(0.2)

Let $p$ denote a prime and let $F_p$ denote the field of size $p$. Campbell, Hughes, and Pollack [1] showed that

$$F_p[1/U_1, U_i, V_i : 1 \leq i \leq m]^\text{UT(Fp)}$$

$$= F_p[1/U_1, U_i, V_i^p - U_i^{p-1} V_i, U_1 V_j - U_j V_1 : 1 \leq i \leq m, 2 \leq j \leq m]$$

(0.3)

and

$$F_p[U_1, U_2, V_1, V_2]^\text{UT(Fp)}$$

$$= F_p[U_1, V_i^p - U_i^{p-1} V_i, U_1 V_2 - U_2 V_1 : i = 1, 2].$$

(0.4)

Let $A$ denote a finite additive subgroup of $K$ (such a subgroup can be non-trivial only when the characteristic of $K$ is non-zero). This paper proves that

if $m \geq 2$ and $|A| > 1$, then $K[U_i, V_i : 1 \leq i \leq m]^\text{UT(A)}$ is generated as a $K$-algebra by polynomials whose degrees are less than or equal to $m(|A| - 1)$

(0.5)

and

if $m \geq 3$, then $K[U_i, V_i : 1 \leq i \leq m]^\text{UT(A)}$ cannot be generated as a $K$-algebra by polynomials whose degrees are strictly less than $m(|A| - 1)$.

(0.6)

This paper also proves that

if $m \geq 3$ and $|A| > 1$, and $S(m)$ is a set of $K$-algebra generators of $K[U_i, V_i : 1 \leq i \leq m]^\text{UT(A)}$, then the monomial $(U_1 V_2 V_3 \cdots V_m)^{|A| - 1}$ appears in some element of $S(m)$.

(0.7)

Note that statement (0.6) is an immediate consequence of statement (0.7). Statement (0.6) implies that if $|A| > 1$ and $m$ is very large, then every set of $K$-algebra generators of $K[U_i, V_i : 1 \leq i \leq m]^\text{UT(A)}$ must contain a generator whose degree is very large. This contrasts with the situations described
in statements (0.2) and (0.3); this also contrasts with the results of E. Noether [11; 18, pp. 275–276] on the invariants of finite groups over fields of characteristic zero.

It is an open problem to concretely list a finite set of $K$-algebra generators of $K[U_i, V_i : 1 \leq i \leq m]^{U_T(A)}$ when $m > 2$ and $A$ is a finite additive subgroup of $K$ whose size is strictly greater than 1. I conjecture that if the characteristic of $K$ is $p$ and $A$ is an additive subgroup of $K$ of size $p$, then

$$
K[U_i, V_i : 1 \leq i \leq m]^{U_T(A)} = K \left[ U_i, \prod_{a \in A} (a U_i + V_i), U_i V_j - U_j V_i, \right.
$$

$$
\sum_{a \in U_T(A)} f^a : 1 \leq i, j \leq m, f
$$

divides $(V_1 V_2 \ldots V_m)^{p-1}$.

This paper establishes the conjecture in the case that $p = 2$.

In order to describe and motivate the results in the last section of the paper, the following definitions and notations are needed. Let $\{C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ denote a set of commuting indeterminates. Let $GL(n, K)$ denote the group of invertible $n \times n$ matrices whose entries lie in $K$. If $g = (g_{ij}) \in GL(n, K)$ and $f \in K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n]$, let $f^g$ denote the image of $f$ under the $K$-algebra homomorphism which maps $C_{ij}$ to $C_{ij} g_{ij} + C_{i2} g_{2j} + \cdots + C_{in} g_{nj}$ for all $i, j$. If $G \subseteq GL(n, K)$, let $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n]^G$ denote the set of elements $f$ in $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq N]$ such that $f^g = f$ for every $g \in G$. Such elements $f$ are called vector invariants (or simply invariants) of $G$ and the ring $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n]^G$ is called the ring of invariants of $G$ acting on $m \times n$-component vectors (the vectors referred to here are the $n$-tuples $(C_{i1}, C_{i2}, \ldots, C_{in})$).

It is easy to verify that if $G$ is a subset of $GL(n, K)$ which contains infinitely many scalar multiples of the identity matrix, then $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n]^G = K$. Therefore, if $K$ is infinite, then $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n]^G_{L(n, K)} = K$. Let $SL(n, K)$ denote the set of matrices in $GL(n, K)$ of determinant 1. It is known that

if $K$ is an infinite field, then $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n]^G_{L(n, K)}$ is generated as a $K$-algebra by the $n \times n$ minors of $(C_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$.

(0.8)

Proofs of this result, in the case that the characteristic of $K$ is 0, can be found in [17, pp. 187–189; 18, pp. 45–47]. Statement (0.8) was first proved in full generality by Igusa [7]; several more elementary proofs have later
appeared, e.g., in [2, 3, 14]. The introduction in [14] contains references to other proofs of statement (0.8). Dickson [5] discovered finite sets of $K$-algebra generators of $K[C_{ij}: 1 \leq j \leq n]^{GL(n, K)}$ and $K[C_{ij}: 1 \leq j \leq n]^{SL(n, K)}$ in the case that $K$ is a finite field. Simpler proofs of these results are found in [6, 13, 19]. Krathwohl [8] discovered generators for the invariants of $GL(2, K)$ acting on two 2-component vectors in the case that $K$ is a finite field. Other results about invariants over finite fields are found in [6; 12; 15; 16; 10, pp. 9-10]. It is an open problem to concretely list a finite set of generators of $K[C_{ij}: 1 \leq i \leq m, 1 \leq j \leq n]^{GL(n, K)}$ or $K[C_{ij}: 1 \leq i \leq m, 1 \leq j \leq n]^{SL(n, K)}$ in the case that $K$ is a finite field, $m > 2$ and $n \geq 2$. This paper establishes the following result.

Let $F$ denote a finite field and let $G \subseteq GL(n, F)$. Let $I$ denote the $n \times n$ identity matrix and suppose that there is an element $g \in GL(n, F)$ such that $\text{rank}(g - I) = 1$, $(g - I)^2 = 0$, and $I + x(g - I) \in G$ for every $x \in F$. If $m > n$, then every set of $F$-algebra generators of $F[C_{ij}: 1 \leq i \leq m, 1 \leq j \leq n]^G$ contains a generator whose degree is greater than or equal to $(m - n + 2)(|F| - 1)$.

(0.9)

Note that if $G$ satisfies the conditions of statement (0.9) and $m$ is much larger than $n$, then every set of generators of the invariants of $G$ must contain a generator whose degree is much larger than $\max\{n, |G|\}$. This contrasts with situation described in statement (0.8) and with the results of Noether [11; 18, pp. 275-276]. Observe that if $n \geq 2$ and $F$ is a finite field, then the groups $SL(n, F)$ and $GL(n, F)$ satisfy the conditions of statement (0.9). Therefore the result stated in the abstract is a consequence of statement (0.9).

For the rest of this paper, let $K$ denote a field of characteristic $p > 0$. Let $A$ denote a finite additive subgroup of $K$ and let $N_A(V_i) = \prod_{a \in A} (aU_i + V_i)$ for $i = 1, 2, \ldots, m$.

This paper is organized as follows. Section 1 contains a proof of statement (0.5) and of a generalization of Eq. (0.3). Section 2 describes properties of monomials which appear in invariants of $UT(A)$. Section 3 contains a proof of statement (0.7). Section 4 contains a proof that $K[U_{ij}, N_A(V_i), U_iV_j - U_jV_i: 1 \leq i, j \leq m]$ contains every element of $K[U_{ij}, V_i: 1 \leq i \leq m]^{UT(A)}$ whose degree is strictly less than $2|A| - |A|/p$. It also contains a proof of a generalization of Eq. (0.4). Section 5 contains examples of invariants of $UT(A)$ and $GL(n, F)$, where $F$ denotes a finite field. Section 6 contains a proof of statement (0.9), based on results from Sections 2 and 3.
1. Examples of Sets of Generators of the Invariants of $UT(A)$

**Proposition 1.** Let $B_m = B_m(A)$ denote the $K$ vector space spanned by the monomials $U_1^{d_1} \ldots U_m^{d_m} V_1^{e_1} \ldots V_m^{e_m}$ such that $d_i + e_i < |A|$ for $i = 1, \ldots, m$. Then

$$K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$$

is generated as a $K[U_i, V_i : 1 \leq i \leq m]_{UT(A)}$-module by $B_m^{UT(A)}$. (1.1)

Therefore $K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$ is generated as a $K$-algebra by polynomials whose degrees are less than or equal to $\max\{|A|, m(|A| - 1)\}$.

**Proof.** Let $W$ denote the $K$ vector spanned by the monomials $U_1^{d_1} \ldots U_m^{d_m} V_1^{e_1} \ldots V_m^{e_m}$ such that $e_i < |A|$ for $i = 1, 2, \ldots, m$.

**Claim.** $K[U_i, V_i : 1 \leq i \leq m]$ is the direct sum of the vector spaces $W_{N_A(V_1)^{e_1}} \ldots N_A(V_m)^{e_m}$, as $(e_1, \ldots, e_m)$ varies over all $m$-tuples of non-negative integers.

**Proof of the Claim.** If $f$ is a non-zero element of $K[U_i, V_i : 1 \leq i \leq m]$, define the $V$-exponent of $f$ to be the lexicographically biggest $m$-tuple $(E_1, \ldots, E_m)$ such that $V_1^{E_1} \ldots V_m^{E_m}$ divides some monomial appearing in $f$. Note that if $f \in W_{N_A(V_1)^{e_1}} \ldots N_A(V_m)^{e_m}$ and $(E_1, \ldots, E_m)$ is its $V$-exponent, then $|A| e_i \leq E_i < |A|(e_i + 1)$ for every $i$. Therefore a collection of non-zero polynomials which lie in distinct vector spaces of the form $W_{N_A(V_1)^{e_1}} \ldots N_A(V_m)^{e_m}$ must have distinct $V$-exponents and hence must be linearly independent over $K$. Therefore the vector spaces $W_{N_A(V_1)^{e_1}} \ldots N_A(V_m)^{e_m}$ are linearly disjoint.

Define the $V$-degree of the monomial $U_1^{d_1} \ldots U_m^{d_m} V_1^{e_1} \ldots V_m^{e_m}$ to be $e_1 + \cdots + e_m$. Let $W^*$ denote the sum of the vector spaces $W_{N_A(V_1)^{e_1}} \ldots N_A(V_m)^{e_m}$, as $(e_1, \ldots, e_m)$ varies over all $m$ tuples of non-negative integers. It will be shown by induction on the $V$-degree that every monomial in $K[U_i, V_i : 1 \leq i \leq m]$ lies in $W^*$. Let $g = U_1^{d_1} \ldots U_m^{d_m} V_1^{E_1} \ldots V_m^{E_m}$. If $E_i < |A|$ for $i = 1, \ldots, m$, then $g \in W$. Suppose now that $E_i \geq |A|$ for some subscript $i$. Write, for $j = 1, \ldots, m$, $E_j = |A| b_j + c_j$, where $b_j$ and $c_j$ are non-negative integers and $c_j < |A|$. Let $w = U_1^{d_1} \ldots U_m^{d_m} V_1^{c_1} \ldots V_m^{c_m}$ and note that $w \in W$. Note also that

$$w_{N_A(V_1)^{b_1}} \ldots N_A(V_m)^{b_m} = g + \text{a linear combination of monomials whose } V \text{-degrees are strictly less than the } V \text{-degree of } g.$$

This equation and the induction hypothesis imply that $g$ lies in $W^*$. Thus
contains every monomial in $K[U_i, V_i : 1 \leq i \leq m]$, so $W^* = K[U_i, V_i : 1 \leq i \leq m]$. This establishes the claim.

For every $\sigma \in UT(A)$ and $i \in \{1, \ldots, m\}$, $N_{A}(V_i)$ is fixed by $\sigma$ and $W$ is mapped into itself by $\sigma$. This observation and the claim imply that

$$K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$$

is the direct sum of the vector spaces $W^{UT(A)} N_{A}(V_1)^{e_1} \cdots N_{A}(V_m)^{e_m}$, as $(e_1, \ldots, e_m)$ varies over all $m$-tuples of non-negative integers.

Let $b_1, \ldots, b_m$ denote non-negative integers. Let $W(b_1, \ldots, b_m)$ denote the $K$ vector space spanned by the monomials $U_1^{d_1} \cdots U_m^{d_m} V_1^{e_1} \cdots V_m^{e_m}$ such that $d_i + e_i = b_i$ and $e_i < |A|$ for $i = 1, \ldots, m$. Note that $W$ is the direct sum of the vector spaces $W(b_1, \ldots, b_m)$, as $(b_1, \ldots, b_m)$ varies over all $m$-tuples of non-negative integers, and

$$W^{UT(A)} = \bigoplus_{(b_1, \ldots, b_m)} W(b_1, \ldots, b_m)^{UT(A)}. \quad (1.3)$$

If $h$ is an integer, define $e(h) = \min\{h, |A| - 1\}$. Observe that, for every $m$-tuple $(b_1, \ldots, b_m)$ of non-negative integers,

$$W(b_1, \ldots, b_m) = \left( \prod_{i=1}^{m} U_i^{b_i - e(b_i)} \right) W(e(b_1), \ldots, e(b_m))$$

and

$$W(b_1, \ldots, b_m)^{UT(A)} = U_1^{b_1 - e(b_1)} \cdots U_m^{b_m - e(b_m)} W(e(b_1), \ldots, e(b_m))^{UT(A)}. \quad (1.4)$$

Note that

$$W(e(b_1), \ldots, e(b_m)) \subset B_m$$

for every $m$-tuple $(b_1, \ldots, b_m)$ of non-negative integers.

Statements (1.2)–(1.5) imply that $K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$ is contained in the $K[U_i, N_{A}(V_i) : 1 \leq i \leq m]$-module generated by $B_m^{UT(A)}$. Therefore statement (1.1) holds. The last assertion of the proposition is an immediate consequence of statement (1.1).

Note that $B_m$ is a finite-dimensional vector space over $K$ and $UT(A)$ is finite. Therefore one can compute a basis for $B_m^{UT(A)}$ by a straightforward linear algebra computation. Hence, by Proposition 1, one can concretely compute a finite set of generators of $K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$.

Proposition 1 can be generalized as follows. Suppose that $g = (a \ b)$, where $a, b, d \in K$ and $ad \neq 0$. For each $f \in K[U_i, V_i : 1 \leq i \leq m]$, let $f^g$ denote the image of $f$ under the $K$-algebra homomorphism which maps $U_i$
to $aU_i$ and $V_i$ to $bU_i + dV_i$ for every $i$. Let $G$ denote a finite subgroup of
\{$(a,b,d) : a, b, d \in K, ad \neq 0 \}$. If $f \in K[U_i, V_i : 1 \leq i \leq m]$, let $N_G(f)$ denote the
product of the elements of $f^g : g \in G$. Let $B_m(G)$ denote the $K$ vector
space spanned by the monomials $U_1^{d_1} \cdots U_m^{d_m} V_1^{e_1} \cdots V_m^{e_m}$ such that $d_i + e_i \leq \deg N_G(U_i) + \deg N_G(V_i) - 2$ for every $i$, and let $B_m(G)^G$ denote the set of
elements of $B_m(G)$ which are invariants of $G$. Then

the set of invariants of $G$ in $K[U_i, V_i : 1 \leq i \leq m]$ is

generated as a $K[N_G(U_i), N_G(V_i) : 1 \leq i \leq m]$-module by

\[ B_m(G)^G. \] (1.6)

This result can be established by an argument similar to the one used to
prove Proposition 1; since the result will not be used in the rest of the
paper, the details of the proof are omitted.

The following proposition describes more explicitly a set of generators of
$K[U_i, V_i : 1 \leq i \leq m]$ in the case that $|A| = 2$.

**Proposition 2.** Assume that the characteristic of $K$ is 2 and let $\sigma$ denote
a non-identity element of $UT(K)$. Then

\[ K[U_i, V_i : 1 \leq i \leq m]^{\{\sigma\}} = K[h + h^\sigma, V_1, V_2 : h \text{ divides } V_1 V_2 \cdots V_m, 1 \leq i \leq m]. \] (2.1)

**Proof.** If $S \subseteq \{1, 2, \ldots, m\}$, define $U_S = \prod_{i \in S} U_i$ and $V_S = \prod_{i \in S} V_i$.
Note that there is a non-zero element $\gamma$ in $K$ such that

\[ V_1^\gamma = V_1 + \gamma U_1 \] for every $i$. (2.2)

Therefore, for every subset $S$ of $\{1, \ldots, m\}$,

\[ g^{1_S} U_S = \prod_{i \in S} (V_1^\gamma + V_i) \]

\[ = \sum_{S^* \subseteq S} V_1^{(S^*)} V_{S - S^*}. \] (2.3)

Let $B_m$ denote the $K$ vector space spanned by $\{U_S V_T : S$ and $T$ are disjoint
subsets of $\{1, \ldots, m\}\}$. Equation (2.3) implies that

\[ B_m \text{ is spanned by } \{V_1^{S^*} V_T : S \text{ and } T \text{ are disjoint subsets of } \{1, \ldots, m\}\}. \] (2.4)

Let $B^* = \{V_1^{S^*} V_T : S \text{ and } T \text{ are disjoint subsets of } \{1, \ldots, m\}\}$. Equation (2.2) implies that the linear forms $V_1, \ldots, V_m, V_1^\gamma, \ldots, V_m^\gamma$ are algebraically
independent over $K$; therefore $B^*$ is a linearly independent set over $K$. The
hypotheses that $\sigma \in \text{UT}(K)$ and the characteristic of $K$ is two imply that $\sigma^2$ is the identity map. Therefore

$$ (V_S^\sigma V_T^\sigma)^\sigma = V_S V_T^\sigma $$

for all subsets $S$, $T$ of \{1, ..., $m$\}. \hspace{1cm} (2.5)

Let $f \in B_m^{[\sigma]}$. Statement (2.4) implies that $f$ can be expressed as a linear combination of elements of $B^\sigma$. Recall that $B^\sigma$ is a linearly independent set; therefore Eq. (2.5) and the fact that $f^\sigma = f$ imply that the coefficient of $V_S^\sigma V_T^\sigma$ in $f$ is the same as that of $V_S V_T^\sigma$ in $f$ for every element $V_S^\sigma V_T^\sigma \in B^\sigma$. Therefore $f$ is a scalar plus a linear combination of the polynomials $V_S V_T^\sigma + V_S^\sigma V_T$, where $V_S^\sigma V_T$ varies over the elements of $B^\sigma$. This proves that

$$ B_m^{[\sigma]} \subset K[V_S V_T + V_S^\sigma V_T^\sigma : S \text{ and } T \text{ are disjoint subsets of } \{1, ..., m\}] \hspace{1cm} (2.6) $$

Suppose that $S$ and $T$ are disjoint subsets of \{1, ..., $m$\}. Observe that

$$ V_S^\sigma V_T + V_S V_T^\sigma = (V_S + V_S^\sigma)(V_T + V_T^\sigma) - (V_S V_T + V_S^\sigma V_T^\sigma) $$

$$ = (V_S + V_S^\sigma)(V_T + V_T^\sigma) - (V_{S \cup T} + V_{S \cup T}^\sigma). $$

This equation and statement (2.6) imply that

$$ B_m^{[\sigma]} \subset K[V_S + V_S^\sigma : 1 \leq i \leq m] \hspace{1cm} (2.7) $$

Since $\sigma^2$ is the identity map, \{identity, $\sigma$\} is a subgroup of $\text{UT}(K)$. Note also that $U_i \in B_m^{[\sigma]}$ for every $i \in \{1, ..., m\}$. Therefore Proposition 1 implies that $K[U_i, V_i : 1 \leq i \leq m]^{[\sigma]}$ is generated as a $K$-algebra by $\{V_i V_i^\sigma : 1 \leq i \leq m\} \cup B_m^{[\sigma]}$. This observation and relation (2.7) establish Eq. (2.1).

**PROPOSITION 3.** If $f \in K[U_i, V_i : 1 \leq i \leq m]^{\text{UT}(A)}$, then

$$ U_i^{m-1} f \in K[U_i V_j - U_j V_i, U_i, N_A(V_i) : 1 \leq i \leq m, 2 \leq j \leq m]. $$

**Proof.** Let $R = K[U_i V_j - U_j V_i, U_i : 1 \leq i \leq m, 2 \leq j \leq m]$. Note that, if $e_1, ..., e_m$ are non-negative integers, then

$$ U_i^{e_i} V_1^{e_1} V_2^{e_2} \cdots V_m^{e_m} = V_1^{e_1} \prod_{i=2}^{m} (U_i V_i - U_i V_i + U_i V_i) V_1^{e_1} \in R[V_1]. \hspace{1cm} (3.1) $$

The claim from the proof of Proposition 1 implies that

$$ K[U_i, V_1] = K[U_i, N_A(V_1)] + K[U_i, N_A(V_1)] V_1 $$

$$ + \cdots + K[U_i, N_A(V_1)] V_1^{[\sigma]-1}. $$
Therefore
\[ R[V_1] \subseteq R[N_A(V_1)] + R[N_A(V_1)] V_1 + \cdots + R[N_A(V_1)] V_1^{|A|-1}. \quad (3.2) \]

Let \( W \) denote the \( K \) vector space spanned by the monomials 
\[ U_1^{e_1} \cdots U_m^{e_m} V_1^{e_1} \cdots V_m^{e_m} \] 
such that \( e_i < |A| \) for every \( i \) and let \( f \) denote an element of \( U_1^{(m-1)(|A|-1)} W^{|UT(A)|} \). Relations (3.1) and (3.2) imply that

\[
\text{there exist elements } r_0, r_1, \ldots, r_{|A|-1} \text{ in } R[N_A(V_1)] \text{ such that } f = r_0 + r_1 V_1 + r_2 V_1^2 + \cdots + r_{|A|-1} V_1^{|A|-1}. \quad (3.3)
\]

Let \( Y \) denote an indeterminate and let \( \sigma \) denote the \( K \)-algebra automorphism of \( K[Y, U_i, V_i : 1 \leq i \leq m] \) such that \( Y^\sigma = Y, U_i^\sigma = U_i, \) and \( V_i^\sigma = YU_i + V_i \) for every \( i \). Since \( f \) is an invariant of \( UT(A) \), \( f^\sigma - f \) becomes zero when \( Y \) is replaced by any element of \( A \). Therefore

\[ f^\sigma - f \text{ is divisible by } \prod_{a \in A} Y - a. \quad (3.4) \]

A similar argument implies that

\[ r^\sigma - r \text{ is divisible by } \prod_{a \in A} Y - a \text{ for every } r \in R[N_A(V_1)]. \quad (3.5) \]

Note that
\[
0 \equiv f^\sigma - f \pmod{\prod_{a \in A} Y - a}, \text{ by } (3.4) \\
\equiv \sum_{i=1}^{|A|-1} r_i ((V_i^\sigma)^i - V_i^i) \pmod{\prod_{a \in A} Y - a}, \text{ by } (3.3) \text{ and } (3.5).
\]

This congruence and the fact that the \( Y \)-degree of \( \sum_{i=1}^{|A|-1} r_i ((V_i^\sigma)^i - V_i^i) \) is strictly less than \( |A| \) imply that \( \sum_{i=1}^{|A|-1} r_i ((V_i^\sigma)^i - V_i^i) = 0 \). This equation and the fact that \( V_i^\sigma \) is transcendental over \( K(U_i, V_i : 1 \leq i \leq m) \) (because \( Y \) is an indeterminate) imply that \( r_i = 0 \) for every \( i > 0 \). This observation and Eq. (3.3) imply that \( f = r_0 \in R[N_A(V_1)] \). This proves (since \( f \) is an arbitrary element of \( U_1^{(m-1)(|A|-1)} W^{|UT(A)|} \)) that \( U_1^{(m-1)(|A|-1)} W^{|UT(A)|} \subseteq R[N_A(V_1)] \). This containment and statement (1.2) imply that

\[ U_1^{(m-1)(|A|-1)} K[U_i, V_i : 1 \leq i \leq m]^{UT(A)} \subseteq R[N_A(V_i) : 1 \leq i \leq m]. \]

This completes the proof. \( \square \)

**Corollary.**

\[ K[U_i, V_i, 1/U_i : 1 \leq i \leq m]^{UT(A)} = K[U_i V_j - U_j V_i, U_i, N_A(V_1), 1/U_i : 1 \leq i \leq m, 2 \leq j \leq m]. \]
Proof. The polynomials $U_j V_j - U_j V_1$, $U_1$, and $N_A(V_1)$ are invariants of $UT(A)$, so

$$K[U_1 V_j - U_j V_1, U_1, N_A(V_1), 1/U_1 : 1 \leq i \leq m, 2 \leq j \leq m]$$

is a subset of $K[U_i, V_i, 1/U_1 : 1 \leq i \leq m]^{UT(A)}$. (3.6)

Suppose that $f \in K[U_i, V_i, 1/U_1 : 1 \leq i \leq m]^{UT(A)}$, then there is an integer $d > 0$ such that $U_1^d f \in K[U_i, V_i, 1 \leq i \leq m]^{UT(A)}$. This observation and Proposition 3 imply that

$$f \in K[U_1 V_j - U_j V_1, U_1, N_A(V_1), 1/U_1 : 1 \leq i \leq m, 2 \leq j \leq m].$$

(3.7)

Define $h(X) = \prod_{a \in A} (X + a)$ and note that

$$N_A(V_i) - U^{\text{deg} h(V_i/U_i)}$$

for every $i$. (3.8)

The theory of $p$-polynomials [13, pp. 564–565] implies that there are elements $c_0, c_1, \ldots, c_e$ in $K$ such that $c_e \neq 0$ and $h(X) = \sum_{j=0}^e c_j X^j$. This observation and Eq. (3.8) imply that

$$N_A(V_i) = \sum_{j=0}^e c_j V_j^p U_j^p - p^i$$

for every $i$. (3.9)

Observe that, for every $i \in \{1, \ldots, m\}$,

$$U_j^{p^i} N_A(V_i) = \sum_{j=0}^e c_j (U_1 V_i)^{p^i} (U_1 U_i)^{p^i - p^j},$$

by (3.9)

$$= \sum_{j=0}^e c_j (U_1 V_i - U_i V_1)^{p^i} (U_1 U_i)^{p^i - p^j} + \sum_{j=0}^e c_j (U_i V_1)^{p^i} (U_1 U_i)^{p^i - p^j}$$

$$= \sum_{j=0}^e c_j (U_1 V_i - U_i V_1)^{p^i} (U_1 U_i)^{p^i - p^j} + U_i^{p^i} N_A(V_1),$$

by (3.9)

$$\in K[U_1 V_i - U_i V_1, U_1, U_i, N_A(V_1)].$$

This observation and statement (3.7) imply that $f \in K[U_1 V_i - U_i V_1, U_1, N_A(V_1), 1/U_1 : 1 \leq i \leq m, 2 \leq j \leq m]$ for every $f \in K[U_i, V_i, 1/U_1 : 1 \leq i \leq m]^{UT(A)}$. This observation and statement (3.6) establish the corollary. \qed
This corollary implies that

the field of fractions of $K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$

equals $K(U_i, U_j V_j - U_j V_1, N_{A}(V_1) : 1 \leq i \leq m, 2 \leq j \leq m)$. \hspace{1cm} (3.10)

Note that every element of $K[U_i, V_i : 1 \leq i \leq m]$ is algebraic over the
field of fractions of $K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$, because $UT(A)$ is a finite

group. Therefore the transcendence degree of the field of fractions of
$K(U_i, V_i : 1 \leq i \leq m)^{UT(A)}$ over $K$ equals the transcendence degree of
$K(U_i, V_i : 1 \leq i \leq m)$ over $K$, which equals $2m$. This observation and state-
ment (3.10) imply that

the set \{ $U_i, U_j V_j - U_j V_1, N_{A}(V_1) : 1 \leq i \leq m, 2 \leq j \leq m$ \}

is algebraically independent over $K$. \hspace{1cm} (3.11)

Statements (3.10) and (3.11) imply that the field of fractions of
$K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$ is a purely transcendental extension of $K$. 

2. PROPERTIES OF MONOMIALS

WHICH APPEAR IN INVARIANTS OF $UT(A)$

The results of this section imply that if $B_m$ is defined as in Proposition 1,
then every non-constant monomial which appears in an element of $B_m^{UT(A)}$
must be divisible by $U_1$ or $U_2$ or ... or $U_m$. Note, however, that a non-
constant monomial which appears in an invariant of $UT(A)$ need not be
divisible by $U_1$ or $U_2$ or ... or $U_m$; for example, the monomial $V_1^{[A]}
appears in $\prod_{a \in A} (V_1 + aU_1)$, which is an invariant of $UT(A)$.

PROPOSITION 4. Let $\Pi_{i=1}^{m} U_i^{d_i} V_i^{e_i}$ denote a monomial which appears in
an invariant of $UT(A)$. If $T$ is a subset of \{ $1, ..., m$ \} such that $d_i = 0$ for every
$t \in T$ and $\sum_{t \in T} e_t < |A|$, then $d_1 + ... + d_m \geq \sum_{t \in T} e_t$.

Proof. First some notation and preliminary observations are intro-
duced. Let $f$ denote an invariant of $UT(A)$ in which $\prod_{i=1}^{m} U_i^{d_i} V_i^{e_i}$ appears.
Let $Y$ denote an indeterminate and let $f^*$ denote the image of $f$ under the
$K$ algebra homomorphism which maps $U_i$ to $U_i$ and $V_i$ to $YU_i + V_i$, for
every $i$. Write

$$f^* = \sum_{w} \sum_{i=0}^{\deg f} c(w, i) w^{Y_i},$$

where the outer sum ranges over all monomials $w$ in $K[U_i, V_i : 1 \leq i \leq m]$
whose degrees do not exceed $\deg f$ and $c(w, i) \in K$ for all $w, i$. Observe
that if \( Y \) is replaced by zero, then \( f^* \) is replaced by \( f \). Therefore

\[
f^* - f = \sum_{w} \sum_{i=1}^{\deg f} c(w, i) w Y'.
\]

(4.1)

The next goal is to express the coefficients \( c(w, i) \), which appear in Eq. (4.1), in terms of the coefficients of \( f \). Suppose that \( h \) is a map from \( \{1, \ldots, m\} \) to the integers such that \( 0 \leq h(i) \leq d_i + e_i \) for every \( i \). Define

\[
\text{mon}(h) = \prod_{i=1}^{m} U_i^{d_i + e_i - h(i)} Y_i^{h(i)}.
\]

If \( j \geq 0 \), let \( M^*(h, j) \) denote the set of maps \( g \) from \( \{1, \ldots, m\} \) to the integers such that \( d_i + e_i \geq g(i) \geq h(i) \) for every \( i \), and \( g(1) + g(2) + \cdots + g(m) = h(1) + h(2) + \cdots + h(m) + j \). The definition of \( f^* \) implies that

\[
c(\text{mon}(h), j) = \left( \prod_{i=1}^{m} \binom{g(i)}{h(i)} \right) \text{(the coefficient of mon}(g) \text{ in } f) \]

(4.2)

for every integer \( j \geq 0 \); here \( \binom{g(i)}{h(i)} \) denotes the binomial coefficient.

Let \( T \) denote a subset of \( \{1, \ldots, m\} \) such that \( d_t = 0 \) for every \( t \in T \) and \( \sum_{t \in T} e_t < |A| \). Let \( M(h, j) \) denote the set of maps \( g \) from \( \{1, \ldots, m\} \) to the integers such that \( g(i) = h(i) \) for every \( i \in \{1, \ldots, m\} - T \), \( 0 \leq g(t) \leq e_t \) for every \( t \in T \), and \( \sum_{t \in T} g(t) = j \). The proposition will be derived from the following claim.

Claim. If \( j > \sum_{i \in \{1, \ldots, m\} - T} (d_i + e_i - h(i)) \), then

\[
\sum_{g \in M(h, j)} \text{the coefficient of mon}(g) \text{ in } f = 0.
\]

Proof of the Claim. Let \( u(h) = \sum_{i \in \{1, \ldots, m\} - T} (d_i + e_i - h(i)) \) and suppose that \( j > u(h) \); the claim will be established by induction on \( u(h) \). Observe that neither \( u(h) \) nor \( M(h, j) \) depends on the restriction of \( h \) to \( T \). Therefore we may assume without loss of generality that \( h(t) = 0 \) for every \( t \in T \). Using this assumption, it will be shown that

\[
c(\text{mon}(h), j) = \sum_{g \in M(h, j)} \text{the coefficient of mon}(g) \text{ in } f.
\]

(4.3)

Assume at first and \( u(h) = 0 \). This assumption and the fact that \( h(i) \leq d_i + e_i \) for every \( i \) imply that \( h(i) = d_i + e_i \) for every \( i \in \{1, \ldots, m\} - T \). This observation and the assumption that \( h(t) = 0 \) for every \( t \in T \) imply that
$M^*(h, j) = M(h, j)$ and $\prod_{i=1}^m \left(\frac{g(i)}{h(i)}\right) = 1$ for every $g \in M^*(h, j)$. Therefore Eq. (4.3) follows immediately from Eq. (4.2).

Suppose now that $u(h) > 0$. Note that $M(h, j) \subseteq M^*(h, j)$, because $h(t) = 0$ for every $t \in T$. Equation (4.2) and the assumption that $h(t) = 0$ for every $t \in T$ imply that

$$c(\text{mon}(h), j) = \sum_{g \in M(h, j)} \text{the coefficient of mon}(g) \text{ in } f$$

+ a linear combination of expressions of the form

$$\sum_{g \in M(z, k)} \text{the coefficient of mon}(g) \text{ in } f,$$

where

$$d_i + e_i \geq z(i) \geq h(i) \text{ for every } i, z(t) = 0 \text{ for every } t \in T, \sum_{i=1}^m z(i) > \sum_{i=1}^m h(i), \text{ and}

k + \sum_{i=1}^m z(i) = j + \sum_{i=1}^m h(i).$$

(4.4)

Suppose that $z$ and $k$ satisfy the conditions of statement (4.4). Note that $u(z) < u(h)$, because $\sum_i z(i) > \sum_i h(i)$ and $z(t) = h(t) = 0$ for every $t \in T$. Note also that

$$u(z) = u(h) + \sum_{i=1}^m (h(i) - z(i)),$$

because $z(t) = h(t) = 0$ for every $t \in T$

$$< k, \text{ because } u(h) < j \text{ and } k + \sum_{i=1}^m z(i) = j + \sum_{i=1}^m h(i).$$

Thus $u(z) < u(h)$ and $u(z) < k$; therefore the induction hypothesis for the claim implies that

$$\sum_{g \in M(z, k)} \text{the coefficient of mon}(g) \text{ in } f = 0.$$

This equation and statement (4.4) establish Eq. (4.3). Thus Eq. (4.3) holds in all cases.

Let $E = \sum_{t \in T} (d_t + e_t) = \sum_{t \in T} e_t$. The definition of $M(h, J)$ implies that

$$M(h, J) \text{ is empty when } J > E.$$

(4.5)

If $u(h) \geq E$, then $j > E$ (by the hypothesis that $j > u(h)$), so statement (4.5) implies that $M(h, j)$ is empty. Therefore the claim is true when $u(h) \geq E$. 

Suppose now that \( u(h) < E \). Equation (4.3) holds for every integer \( j > u(h) \), so it holds for every integer \( j \geq E \) (because \( E > u(h) \)). Therefore Eq. (4.3) (with \( j \) replaced by \( J \)) and statement (4.5) imply that

\[
c(\text{mon}(h), J) = 0 \quad \text{when} \quad J > E.
\]

Recall the definition of \( f^* \). Since \( f \) is an invariant of \( UT(A) \), \( f^* - f \) becomes zero when \( Y \) is replaced by any element of \( A \). Therefore \( f^* - f \) is divisible by \( \prod_{a \in A} Y - a \). This observation and Eq. (4.1) imply that

\[
\sum_{i \geq 1} c(\text{mon}(h), i) Y^i \text{ is divisible by } \prod_{a \in A} Y - a.
\]

Note that

\[
\deg \left( \sum_{i \geq 1} c(\text{mon}(h), i) Y^i \right) \leq E, \quad \text{by (4.6)}
\]

\[
< |A|, \quad \text{by the definitions of } E \text{ and } T.
\]

This inequality and statement (4.7) imply that \( c(\text{mon}(h), i) = 0 \) for every \( i \geq 1 \). In particular, \( c(\text{mon}(h), j) = 0 \). This observation and Eq. (4.3) establish the claim.

Suppose now that \( h(i) = e_i \) for every \( i \in \{1, \ldots, m\} - T \) and \( h(t) = 0 \) for every \( t \in T \). As in the proof of the claim, let \( E = \sum_{i \in T} (d_i + e_i) = \sum_{i \in T} e_i \).

Note that \( M(h, E) \) contains only one element, and

\[
\sum_{g \in M(h, E)} \text{ the coefficient of } \text{mon}(g) \text{ in } f = \text{ the coefficient of } \prod_{i=1}^{m} U_i^{d_i} V_i^{e_i} \text{ in } f
\]

\[
\neq 0, \quad \text{by the definition of } f.
\]

This observation and the claim imply that

\[
E \leq \sum_{i \in \{1, \ldots, m\} - T} (d_i + e_i - h(i)).
\]

Note also that

\[
\sum_{i \in \{1, \ldots, m\} - T} (d_i + e_i - h(i)) = \sum_{i \in \{1, \ldots, m\} - T} d_i \quad \text{by the definition of } h
\]

\[
= d_1 + \cdots + d_m \quad \text{by the definition of } T.
\]

Therefore \( E \leq d_1 + \cdots + d_m \); this establishes the proposition. \( \square \)
PROPOSITION 5. Let $\prod_{i=1}^{m} U_i^d V_i^{e_i}$ denote a monomial which appears in an invariant of $UT(A)$ and let $b$ denote an integer such that $p^b \leq |A|$. If $e_i < p^b$ for every $i$, then $d_i + \cdots + d_m \geq \min\{ |A| - p^{b-1}, e_1 + \cdots + e_m \}$.

Proof: Suppose that $e_i < p^b$ for every $i$, and let $f$ denote an invariant of $UT(A)$ in which $\prod_{i=1}^{m} U_i^d V_i^{e_i}$ appears. Let $\psi$ denote the $K$-algebra homomorphism from $K[U_i, V_i : 1 \leq i \leq m]$ to $K[U_i, V_i : 1 \leq i \leq m + pm]$ such that

$$\psi(U_i) = U_i + U_{i+m} + U_{i+2m} + \cdots + U_{i+pm},$$

and

$$\psi(V_i) = V_i + V_{i+m} + V_{i+2m} + \cdots + V_{i+pm}$$

for every $i \in \{1, \ldots, m\}$. Note that, for every $i \in \{1, \ldots, m\}$ and $\sigma \in UT(A)$, $\psi(U_i) = \psi(U_i^\sigma)$ and $\psi(V_i) = \psi(V_i^\sigma)$. Therefore $\psi(h)^\sigma = \psi(h)\sigma$ for every $h \in K[U_i, V_i : 1 \leq i \leq m]$ and $\sigma \in UT(A)$; hence

$$\psi$$ maps invariants of $UT(A)$ to invariants of $UT(A)$. (5.1)

Claim. There exist integers $c_m + 1, c_{m+2}, \ldots, c_{m+pm}$ such that $0 \leq c_i \leq p^{b-1}$ for every $i$, $c_{m+1} + c_{m+2} + \cdots + c_{m+pm} = e_1 + \cdots + e_m$, and $(\prod_{i=1}^{m} U_i^d)(\prod_{i=m+1}^{m+pm} V_i^{e_i})$ appears in $\psi(f)$.

Proof of the Claim. For every $i \in \{1, \ldots, m\}$, one can write $e_i = a_i p^b + r_i$, where $a_i \in \{0, 1, \ldots, p-1\}$ (because $e_i < p^b$) and $0 \leq r_i < p^{b-1}$. Observe that

$$\psi(V_i)^{a_i p^b + r_i} = (V_i^{p^b + r_i} + V_{i+m}^{p^b + r_i} + \cdots + V_{i+pm}^{p^b + r_i})^a (V_i + \cdots + V_{i+pm})^{r_i},$$

because the characteristic of $K$ is $p$.

This equation and the multinomial theorem (together with the fact that $r_i < p^{b-1}$) imply that the coefficient of $(\prod_{i=1}^{m} V_i^{p^{b-1}}) V_i^r$ in $\psi(V_i)^{a_i}$ is $a_i$. Therefore (since $a_i < p$) the monomial $(\prod_{i=1}^{m} V_i^{p^{b-1}}) V_i^r$ appears in $\psi(V_i)^{a_i}$. Therefore, setting $w_i = (\prod_{i=1}^{m} V_i^{p^{b-1}}) V_i^r$, the monomial $\prod_{i=1}^{m} U_i^{d_i} w_i$ appears in $\psi(\prod_{i=1}^{m} U_i^{d_i} V_i^{e_i})$. Note also that if $h$ is a monomial in $K[U_i, V_i : 1 \leq i \leq m]$ which is different than $\prod_{i=1}^{m} U_i^{d_i} V_i^{e_i}$, then $\prod_{i=1}^{m} U_i^{d_i} w_i$ does not appear in $\psi(h)$. These observations and the hypothesis that $\prod_{i=1}^{m} U_i^{d_i} V_i^{e_i}$ appears in $f$ imply that $\prod_{i=1}^{m} U_i^{d_i} w_i$ appears in $\psi(f)$. This establishes the claim, because one can write $\prod_{i=1}^{m} U_i^{d_i} w_i = \prod_{j=m+1}^{m+pm} V_j^{e_j}$, where the exponents $c_j$ have the desired properties.
Suppose that \( c_{m+1}, c_{m+2}, \ldots, c_{m+pm} \) have the properties stated in the claim. The claim and statement (5.1) imply that

\[
\left( \prod_{i=1}^{m} U_i^{d_i} \right) \left( \prod_{i=m+1}^{m+pm} V_i^{e_i} \right)
\]

appears in an invariant of \( \text{UT}(A) \). \( \text{(5.2)} \)

Let \( T \) denote a maximal subset of \( \{ m+1, m+2, \ldots, m+pm \} \) such that \( \sum_{i \in T} c_i < |A| \). Proposition 4 and statement (5.2) imply that

\[
d_1 + \cdots + d_m \geq \sum_{i \in T} c_i.
\] \( \text{(5.3)} \)

Suppose at first that \( \sum_{i \in T} c_i < c_{m+1} + c_{m+2} + \cdots + c_{m+pm} \). Then there is a subscript \( j \) such that \( c_j > 0 \) and \( j \) does not lie in \( T \). Observe that

\[
\sum_{i \in T} c_i \geq |A| - c_i,
\]

by the maximality of \( T \)

\[
\geq |A| - p^{b-1},
\]

because \( c_i \leq p^{b-1} \) for every \( i \).

Suppose now that \( \sum_{i \in T} c_i = c_{m+1} + c_{m+2} + \cdots + c_{m+pm} \). Then \( \sum_{i \in T} c_i = e_1 + \cdots + e_m \), because \( c_{m+1} + \cdots + c_{m+pm} = e_1 + \cdots + e_m \). Thus, in all cases, \( \sum_{i \in T} c_i \geq \min \{|A| - p^{b-1}, e_1 + \cdots + e_m\} \). This inequality and relation (5.3) imply that \( d_1 + \cdots + d_m \geq \min \{|A| - p^{b-1}, e_1 + \cdots + e_m\} \).

**Remarks.** Let \( f \) and \( \psi \) be defined as in the proof of Proposition 5 (it is not necessary to assume that \( e_i < p^{b} \) for every \( i \)). Note that \( \prod_{i=1}^{m} U_i^{d_i} V_i^{e_i} \) appears in \( \psi(f) \) and \( \psi(f) \) is an invariant of \( \text{UT}(A) \) (by (5.1)). These observations imply (by applying Proposition 4 to \( \prod_{i=1}^{m} U_i^{d_i} V_i^{e_i} \) rather than to \( \prod_{i=1}^{m} U_i^{d_i} V_i^{e_i} \)) that Proposition 4 still holds when one omits the condition that \( d_i = 0 \) for every \( i \in T \).

It will be shown in Remark 3 after Proposition 12 that the lower bound for \( d_1 + \cdots + d_m \) given in Proposition 5 is attained in infinitely many cases.

### 3. Monomials Which Must Appear in Some Generator of the Invariants of \( \text{UT}(A) \)

**Definition.** If \( w = U_1^{d_1} \cdots U_m^{d_m} V_1^{e_1} \cdots V_m^{e_m} \), define the \( U \)-degree of \( w \), denoted by \( U \)-degree \( w \), to be \( d_1 + \cdots + d_m \), and define its \( V \)-degree to be \( e_1 + \cdots + e_m \).

**Proposition 6.** Assume that \( |A| > 1 \). Let \( S \subseteq K[U_i, V_i : 1 \leq i \leq m]^{\text{UT}(A)} \) and let \( K[S] \) denote the \( K \)-algebra which is generated by \( S \). If the monomial \( V_1^{e_1} \) appears in an element of \( K[S] \), then it appears in an element of \( S \). If
the monomial \((U_1 V_2 V_3 \cdots V_k)^{|A| - 1}\), where \(k \geq 3\), appears in an element of \(K[S]\), then it appears in an element of \(S\).

Proof. Suppose that \(V_1^{|A|}\) appears in an element of \(K[S]\). Then one can write

\[
V_1^{|A|} = w_1 w_2 \cdots w_t,
\]

where each \(w_i\) is a non-constant monomial which appears in an element of \(S\). (6.1)

Let \(F_p\) denote the subfield of \(K\) of size \(p\). Since \(A\) is an additive subgroup of \(K\), it is a vector space over \(F_p\). Therefore \(|A|\) is a power of \(p\). Proposition 5, with \(p^h = |A|\), implies that every non-constant monomial which appears in an invariant of \(UT(A)\) and whose degree is strictly less than \(|A|\) must be divisible by \(U_1\) or \(U_2\) or \(\cdots\) or \(U_m\). This observation and Eq. (6.1) imply that \(\deg w_i \geq |A|\) for every \(i\); hence \(t = 1\). Therefore \(V_1^{|A|} = w_1\), so it appears in an element of \(S\).

Suppose now that the monomial \((U_1 V_2 V_3 \cdots V_k)^{|A| - 1}\), where \(k \geq 3\), appears in an element of \(K[S]\). Then one can write

\[
(U_1 V_2 V_3 \cdots V_k)^{|A| - 1} = w_1 w_2 \cdots w_t,
\]

where each \(w_i\) is a non-constant monomial which appears in an element of \(S\). (6.2)

Equation (6.2) implies that there is a subscript \(I\) such that

\[
(U\text{-degree } w_I)/\deg w_I \leq \frac{U\text{-degree}(U_1 V_2 \cdots V_k)^{|A| - 1}}{\deg(U_1 V_2 \cdots V_k)^{|A| - 1}} = \frac{1}{k}\]

\[
\leq \frac{1}{3}, \quad \text{because } k \geq 3.
\]

Therefore

\[
U\text{-degree } w_I \leq (\deg w_I)/3 = (U\text{-degree } w_I + V\text{-degree } w_I)/3.
\]

Therefore \(U\text{-degree } w_I \leq (V\text{-degree } w_I)/2\). This inequality and the fact that \(U\text{-degree } w_I + V\text{-degree } w_I = \deg w_I > 0\) imply that \(U\text{-degree } w_I < V\text{-degree } w_I\). Therefore Proposition 5, with \(p^h = |A|\), implies that

\[
U\text{-degree } w_I \geq |A| - |A|/p. \quad (6.3)
\]

Equation (6.2) implies that one can write \(w_I = U_1^c V_2^{e_2} \cdots V_k^{e_k}\), where \(0 \leq c < |A|\) and \(0 \leq e_i < |A|\) for every \(i\). Define

\[
z = U_1^{|A| - 1 - c} V_2^{|A| - 1 - e_2} V_3^{|A| - 1 - e_3} \cdots V_k^{|A| - 1 - e_k}.\]
Let $e_j = \max\{e_2, ..., e_k\}$ and observe that

$$|A| - 1 \geq e_j \geq \left(\sum_{i=2}^{k} e_i\right)/(k-1)$$

$$= |A| - 1 - (\deg z - U\text{-degree } z)/(k-1).$$

These inequalities and Proposition 4 (with $\prod_{i=1}^{m} U_i^j V_i^{-i} = w_i$ and $T = \{j\}$) imply that

$$U\text{-degree } w_i \geq e_j \geq |A| - 1 - (\deg z - U\text{-degree } z)/(k-1). \quad (6.4)$$

Note that

$$|A| - 1 = U\text{-degree } w_i + U\text{-degree } z, \quad \text{by the definition of } z$$

$$\geq |A| - 1 - (\deg z)/(k-1) + k(U\text{-degree } z)/(k-1), \quad \text{by } (6.4).$$

Therefore

$$k(U\text{-degree } z) \leq \deg z. \quad (6.5)$$

Statements (6.2) and (6.3) imply that, when $i \neq I$, $U\text{-degree } w_i < |A|/p$.

This observation and Proposition 5 (with $p^h = |A|$) imply that $U\text{-degree } w_i \geq V\text{-degree } w_i$ when $i \neq I$; hence

$$2(U\text{-degree } w_i) \geq U\text{-degree } w_i + V\text{-degree } w_i$$

$$= \deg w_i \quad \text{when } i \neq I.$$

Note also that $z = \prod_{i \neq I} w_i$ (by (6.2) and the definition of $z$); therefore

$$2(U\text{-degree } z) \geq \deg z. \quad (6.6)$$

Note that

$$\frac{(\deg z)}{3} \geq \frac{(\deg z)}{k}, \quad \text{because } k \geq 3$$

$$\geq \frac{(\deg z)}{2}, \quad \text{by } (6.5) \text{ and } (6.6).$$

Hence $\deg z = 0$. Note that $(U_1 V_2 V_3 \cdots V_k)^{|A|-1} = w_I$, because $\deg z = 0$. Therefore the monomial $(U_1 V_2 V_3 \cdots V_k)^{|A|-1}$ appears in an element of $S$. \]

**Proposition 7.** If $|A| > 1$ then $\sum_{a \in A} a^{|A|-1} = \prod_{a \in A \setminus \{0\}} a$.

**Proof.** 1. Assume that $|A| > 1$. Define $s(j) = \sum_{a \in A} a^j$ for every integer $j > 0$. Let $J$ denote the smallest integer such that $J > 0$ and $s(J) \neq 0$; it will be shown that $J = |A| - 1$.  

607/81:1-4
Let $X$ denote an indeterminate and define $h(X) = \prod_{a \in A} (1 + aX)$. Taking the formal logarithmic derivative of $h(X)$ yields

$$h'(X)/h(X) = \sum_{a \in A} a/(1 + aX)$$

$$= \sum_{j \geq 0} s(j + 1)(-X)^j. \quad (7.1)$$

Let $f(X) = \prod_{a \in A} (X + a)$ and observe that

$$h(X) = \prod_{a \in A} X(X^{-1} + a) = X^{|A|} f(1/X). \quad (7.2)$$

If $b \in A$, then

$$f'(-b) = \prod_{a \in A - \{b\}} (-b + a) = \prod_{a \in A - \{0\}} a;$$

the last equality is due to the fact that the map $a \mapsto -b + a$ is a one-to-one correspondence from $A - \{b\}$ to $A - \{0\}$. Thus $f'(-b) - \prod_{a \in A - \{0\}} a = 0$ for every $b \in A$; on the other hand, the $X$-degree of $f'(X) - \prod_{a \in A - \{0\}} a$ is strictly less than $|A|$, so

$$f'(X) = \prod_{a \in A - \{0\}} a = f'(0). \quad (7.3)$$

Therefore

$$f(X) = f'(0)X + \text{an element of } K[X^p].$$

This equation and the fact that $\deg f = |A| > 1$ imply that

$$\deg f \text{ and } |A| \text{ are divisible by } p \quad (7.4)$$

and

$$X^{|A|} f(1/X) = f'(0)X^{|A| - 1} + \text{an element of } K[X^p]. \quad (7.5)$$

Note that

$$h'(X) = (|A| - 1) f'(0)X^{|A| - 2}, \quad \text{by (7.2) and (7.5) and}$$

the fact that the characteristic of $K$ is $p$

$$= -f'(0)X^{|A| - 2}, \quad \text{by (7.4).}$$
This equation and Eq. (7.1) imply that

\[ -f'(0)X^{\lvert A \rvert - 1} = h(X) \sum_{j \geq 0} s(j + 1)(-X)^j \]

\[ = h(0) s(J)(-X)^{J - 1} + \text{a power series which is divisible by } X^J. \]

By comparing the lowest powers of \( X \) on each side of this equation and using the fact that \( h(0) = 1 \), one concludes that

\[ |A| - 2 = J - 1 \quad \text{and} \quad f''(0) = (-1)^J s(J). \quad (7.6) \]

The map \( u \mapsto -u \) is a permutation of \( A - \{0\} \), so

\[ \prod_{u \in A - \{0\}} a = \prod_{u \in A - \{0\}} (-a) = (-1)^{|A| - 1} \prod_{u \in A - \{0\}} a. \]

This equation and statement (7.6) imply that

\[ 1 = (-1)^{|A| - 1} = (-1)^J = f''(0)/s(J) = f''(0)/s(|A| - 1). \]

Hence \( f''(0) = s(|A| - 1) \); this equation and Eq. (7.3) imply that

\[ \prod_{u \in A - \{0\}} a = s(|A| - 1). \]

This establishes the proposition. \( \blacksquare \)

Remark. Another way to establish statements (7.3) and (7.4) is to use the theory of \( p \)-polynomials, due to O. Ore [13, pp. 564–565].

Proof 2. Let \( F_p \) denote the subfield of \( K \) of size \( p \). Assume that \( |A| > 1 \) and let \( N \) denote the size of a minimal set of generators of \( A \) as an additive group. Let \( X_1, \ldots, X_N \) denote commuting indeterminates and let \( A^* \) denote the \( F_p \) vector space spanned by \( \{X_1, \ldots, X_N\} \). It will be shown that

\[ \sum_{a \in A^*} a^{|A^*| - 1} = \prod_{a \in A^* - \{0\}} a. \quad (7.7) \]

Note that both \( A \) and \( A^* \) are \( N \)-dimensional vector spaces over \( F_p \). Consider an \( F_p \)-algebra homomorphism from \( F_p[X_1, \ldots, X_N] \) to \( K \) which maps \( \{X_1, \ldots, X_N\} \) to a set of generators of \( A \); by applying such a homomorphism to both sides of Eq. (7.7), one obtains the equation stated in the proposition. Therefore, to finish the proof, it suffices to establish Eq. (7.7).

Let \( L \) denote the left side of Eq. (7.7) and let \( B \) denote the set of linear forms in \( F_p[X_2, \ldots, X_N] \). Observe that when \( X_1 \) is replaced by 0, \( L \) is replaced by \( p \sum_{a \in B} a^{|A^*| - 1} \), which equals 0 because the characteristic of \( F_p \) is \( p \). Hence

\[ L \text{ is divisible by } X_1. \quad (7.8) \]
Observe that if $X_i$ is replaced by $cX_i$, where $c \in F_p - \{0\}$, then $L$ is unchanged. Therefore, if $X_1^{e_1} \cdots X_N^{e_N}$ is any monomial which appears in $L$, then $c^{e_i} = 1$ for every $c \in F_p - \{0\}$; hence $e_i$ must be divisible by $p - 1$. This observation and statement (7.8) imply that

$$L \text{ is divisible by } X_i^{p-1}. \quad (7.9)$$

Note that $L$ is fixed by every automorphism of $F_p[X_1, \ldots , X_N]$ which maps $\{X_1, \ldots , X_N\}$ to a set of linear forms, because such an automorphism permutes the elements of $A^*$. This observation and statement (7.9) imply that $L$ is divisible by $a^{p-1}$ for every non-zero $a \in A^*$. Note also that the least common multiple of the elements of $\{a^{p-1} : a \in A^* - \{0\}\}$ is $\prod_{a \in A^* - \{0\}} a$; hence $L$ is divisible by $\prod_{a \in A^* - \{0\}} a$. This observation and the fact that $\deg L \leq |A^*| - 1 = \deg \prod_{a \in A^* - \{0\}} a$ imply that there exists an element $c \in F_p$ such that $L = c \prod_{a \in A^* - \{0\}} a. \quad (7.10)$

Let $F$ denote a finite field of size $p^N$ (it is shown in [4, Chap. 2, pp. 14-19] that such a field exists). It is known [4, Chap. 1, p. 11] that

$$x^{|F|-1} = 1 \quad \text{for every } x \in F - \{0\}. \quad (7.11)$$

Let $h$ denote a ring homomorphism from $F_p[X_1, \ldots , X_N]$ to $F$ that maps $\{X_1, \ldots , X_N\}$ to a basis for $F$ over $F_p$. Note that the restriction of $h$ to $A^*$ is a one-to-one correspondence between $A^*$ and $F$. Therefore

$$h(L) = \sum_{x \in F} x^{|F|-1} \quad (7.12)$$

and

$$h\left(\prod_{a \in A^* - \{0\}} a\right) - \prod_{x \in F - \{0\}} x. \quad (7.13)$$

By pairing the elements of $F - \{0, -1, 1\}$ with their multiplicative inverses, one obtains the well-known identity

$$\prod_{x \in F - \{0\}} x = -1. \quad (7.14)$$

Note that

$$h(L) = -1, \quad \text{by (7.11) and (7.12)}$$

and

$$= h\left(\prod_{a \in A^* - \{0\}} a\right), \quad \text{by (7.13) and (7.14)}. $$
This equation implies that the scalar $c$ appearing in Eq. (7.10) equals 1. Therefore Eq. (7.7) holds.

Remarks. A shorter (but less self-contained) proof of statement (7.10) can be given by using Dickson’s theorem \cite{5, 6, 13, 19;} on the invariants of $GL(N, F_p)$.

Let $\{a_1, \ldots, a_N\}$ denote a minimal set of generators of $A$ as an additive group. Ore \cite{13, Theorem 9, p. 565;} showed that

$$\prod_{a \in A - \{0\}} a = \left( -1 \right)^N \left( \det \begin{pmatrix} a_1 & a_2 & \cdots & a_N \\ a_1^p & a_2^p & \cdots & a_N^p \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{p^N-1} & a_2^{p^N-1} & \cdots & a_N^{p^N-1} \end{pmatrix} \right)^{p-1}.$$  

This equation can also be derived easily from a result of E. H. Moore \cite{9}.

**Proposition 8.** Assume that $|A| > 1$. Let $S(m)$ denote a set of $K$-algebra generators of $K[U_i, V_i : 1 \leq i \leq m]^{UT(A)}$. If $m \geq 1$, then the monomial $V_i^{[4]}$ appears in some element of $S(m)$, and if $m \geq 3$, then the monomial $(U_1 V_2 V_3 \cdots V_m)^{[4]} - 1$ appears in some element of $S(m)$.

Proof: Note that the monomial $V_i^{[4]}$ appears in $\prod_{a \in A} (V_i + a U_i)$, which is an invariant of $UT(A)$. This observation and Proposition 6 imply that $V_i^{[4]}$ appears in an element of $S(m)$.

Suppose now that $m \geq 3$ and define

$$h = \sum_{a \in A} (V_i + a U_i)^{[4]} - 1 (V_2 + a U_2)^{[4]} - 1 \cdots (V_m + a U_m)^{[4]} - 1.$$  

Note that the coefficient of $(U_1 V_2 V_3 \cdots V_m)^{[4]} - 1$ in $h$ is $\sum_{a \in A} a^{[4]} - 1$, which is non-zero by Proposition 7. Thus the monomial $(U_1 V_2 V_3 \cdots V_m)^{[4]} - 1$ appears in $h$, which is an invariant of $UT(A)$. This observation and Proposition 6 imply that $(U_1 V_2 V_3 \cdots V_m)^{[4]} - 1$ appears in an element of $S(m)$.

**Proposition 9.** Let $R = K[U_i, U_i V_j - U_j V_i : 1 \leq i, j \leq m]$ and let $R^*$ denote the $R$-module which is generated by $\{V_1^{e_1} V_2^{e_2} \cdots V_m^{e_m} : e_1 + \cdots + e_m < |A|\}$. Then $(R^*)^{UT(A)} = R$.
Proof. The polynomials $U_i$ and $U_iV_j - U_jV_i$ are invariants of $\text{UT}(A)$, so

\[\text{every element of } R \text{ is an invariant of } \text{UT}(A). \quad (9.1)\]

Let $Y$ denote an indeterminate and let $\sigma$ denote the $K$-algebra automorphism of $K[Y, U_i, V_i : 1 \leq i \leq m]$ such that $Y^\sigma = Y$, $U_i^\sigma = U_i$, and $V_i^\sigma = YU_i + V_i$ for every $i$. Every element of $R$ is fixed by $\sigma$; therefore

\[\text{for every } f \in R^*, \text{ there exist polynomials } f_0, f_1, \ldots, f_{|A|-1} \text{ in } K[U_i, V_i : 1 \leq i \leq m] \text{ such that } f^\sigma = f_0 + f_1Y + \cdots + f_{|A|-1}Y^{|A|-1}. \quad (9.2)\]

Suppose that $f \in (R^*)^{\text{UT}(A)}$. If $Y$ is replaced by an element of $A$, then $f^\sigma - f$ becomes 0, because $f$ is an invariant of $\text{UT}(A)$. Therefore $f^\sigma - f$ is divisible by $\prod_{u \in A} Y - a$. This observation and statement $(9.2)$ imply that $f^\sigma = f$. Therefore $f$ is an invariant of $\text{UT}(K^*)$ for every field $K^*$ containing $K$. This observation, with $K^* = K(Y)$, and statement $(0.1)$ (with $K$ replaced by $K(Y)$) imply that $f \in K[Y][U_i, U_iV_j - U_jV_i : 1 \leq i, j \leq m]$. Therefore there is a monic polynomial $d(Y) \in K[Y]$ and elements $r_0, r_1, \ldots, r_\ell$ in $R$ such that

\[d(Y)f = r_0 + r_1Y + \cdots + r_\ell Y^\ell.\]

By comparing the coefficients of the highest power of $Y$ on each side of this equation, and recalling that $d(Y)$ is monic, one obtains $f = r_{\deg d(Y)} \in R$. This proves that $(R^*)^{\text{UT}(A)} \subseteq R$. This containment and statement $(9.1)$ establish the proposition.

Recall that $N_A(V_i)$ denotes the polynomial $\prod_{u \in A}(V_i + aU_i)$.

Proposition 10. The algebra $K[U_i, N_A(V_i), U_iV_j - U_jV_i : 1 \leq i, j \leq m]$ contains every element of $K[U_i, V_i : 1 \leq i \leq m]^{\text{UT}(A)}$ whose degree is strictly less than $2|A| - |A|/p$.

Proof. Let $B$ denote the set of polynomials in $K[U_i, V_i : 1 \leq i \leq m]$ whose degrees are strictly less than $2|A| - |A|/p$ and let $W$ denote the $K$ vector spanned by the monomials $U_1^{e_1} \cdots U_m^{e_m}V_1^{c_1} \cdots V_m^{c_m}$ such that $e_i < |A|$ for every $i$. For $i = 1, 2, \ldots, m$, let $W_i$ denote the set of polynomials in $B$ which are divisible by $N_A(V_i)$.

Claim. $B$ is the direct sum of the vector spaces $W \cap B$, $W_1$, $W_2$, ..., $W_m$.

This claim is analogous to the one in the proof of Proposition 1 and can be proved in a similar manner; the details are omitted.
Every automorphism in UT(A) maps $W \cap B$ into itself and $W_i$ into itself for $i = 1, \ldots, m$. This observation and the claim imply that

$$B_{UT (A)}^{m (A)} = \text{the direct sum of } (W \cap B)^{UT (A)}, \ W_0^{UT (A)}, \ W_1^{UT (A)}, \ W_2^{UT (A)}, \ldots, \ W_m^{UT (A)}. \tag{10.1}$$

Observe also that $W_i \subset (W \cap B) N_4 (V_i)$ for every $i$; hence

$$W_i^{UT (A)} \subset (W \cap B)^{UT (A)} N_4 (V_i) \quad \text{for every } i. \tag{10.2}$$

Let $w$ denote a monomial which appears in an element of $(W \cap B)^{UT (A)}$. Proposition 5, with $p^b = |A|$, implies that $U$-degree $w \geq \min \{|A| - |A|/p, \deg w - U$-degree $w\}$, so $U$-degree $w \geq \min \{|A| - |A|/p, \deg w)/2\}$. This observation and the fact that $\deg w < 2 |A| - |A|/p$ (because $w$ appears in an element of $B$) imply that

$$\deg w - U$-degree $w \leq \max \{|A| - 1, \left[(\deg w)/2\right]\} = |A| - 1.$$
Relations (11.1) and (11.2) establish the proposition in the case that $A = A'$.

For brevity let $n_1$ and $n_2$ denote $N.(V_1)$ and $N.(V_2)$, respectively. Suppose that $t \in F_p$; Fermat’s Little Theorem implies that $V_i^p - (xU_i)^{p-1} V_i$ becomes zero when $V_i$ is replaced by $-t x U_i$. Hence $V_i^p - (xU_i)^{p-1} V_i$ is divisible by $V_i + t x U_i$ for every $t \in F_p$; therefore

$$V_i^p - (xU_i)^{p-1} V_i = n_i \quad \text{for } i = 1, 2. \quad (11.3)$$

Therefore

$$U_1 n_2 - U_2 n_1 = (U_1 V_2 - U_2 V_1)^p - (xU_1)^{p-1} (U_1 V_2 - U_2 V_1).$$

This equation can be viewed as an equation of integral dependence of $U_1 V_2 - U_2 V_1$ over $K[U_1, U_2, n_1, n_2]$; hence

$$K[U_1, U_2, n_1, n_2]$$

is generated as a $K[U_1, U_2, n_1, n_2]$-module by $1, U_1 V_2 - U_2 V_1, (U_1 V_2 - U_2 V_1)^p - 1$.

To show $B_2$ denote the $K$ vector space spanned by the monomials $U_1^{d_1} U_2^{d_2} V_1^{e_1} V_2^{e_2}$ such that $d_1 + e_1 < |A|$ and $d_2 + e_2 < |A|$. Let $f$ denote a non-zero element of $B_2^{UT(A)}$; it will be shown that $f \in K[U_1, U_2, U_1 V_2 - U_2 V_1]$. Since $f$ is an invariant of $UT(A)$ and $A \supseteq A'$, it is an invariant of $UT(A')$. This observation and statements (11.1) and (11.4) imply that one can write

$$f = \sum_{I \geq 0} \sum_{J \geq 0} c_{I,J} n_1^J n_2^J,$$

where every $c_{I,J}$ lies in the $K[U_1, U_2]$-module generated by $1, U_1 V_2 - U_2 V_1, ..., (U_1 V_2 - U_2 V_1)^{p-1}$.

Define $e = \max\{i + j : c_{I,J} \neq 0\}$ and let $I$ denote the biggest integer such that $0 \leq I \leq e$ and $c_{e-I,J} \neq 0$. Equations (11.3) and (11.5) and the definitions of $e$ and $I$ imply that

$$f = c_{e-I,J} n_1^J n_2^{e-I} + \text{a polynomial whose } V_1\text{-degree is}
\text{strictly less than } pI + \text{a polynomial whose } V_2\text{-degree is}
\text{strictly less than } p(e-I).$$

Therefore $V_2$-degree $f \geq V_2$-degree $n_2^{e-I} = p(e-I)$ and $V_1$-degree $f \geq V_1$-degree $n_1^I = pI$. These observations and the hypothesis that that $f \in B_2$ imply that

$$p(e-I) < |A| \quad \text{and} \quad pI < |A|. \quad (11.6)$$

The next goal is to show that $I = e$. Let $Y$ denote an indeterminate and
let $f^*$ denote the image of $f$ under the $K$-algebra homomorphism which maps $U_i$ to $U_i$ and $V_i$ to $V_i + YU_i$ for every $i$. Define

$$f^*(i, j) = c_0(n_1 + (Y^p - x^p - 1)U_1)U_2j(n_2 + (Y^p - x^p - 1)U_2)$$

for all $i, j \geq 0$. Equations (11.3) and (11.5) imply that

$$f^* = \sum_i \sum_j f^*(i, j).$$

(11.7)

Observe that

if $i < I$, then the $V_1$-degree of every monomial which appears in $f^*(i, j)$ is strictly less than $pI$

(11.8)

and

if $i + j < e$, then the sum of the $V_1$-degree and $Y$-degree of each monomial which appears in $f^*(i, j)$ is strictly less than $pe$.

(11.9)

Note also that

$$f^*(I, e - I) = c_{i, e - I} V_1^p(YU_2)^{p(e - I)} + \text{a polynomial whose } V_1\text{-degree is strictly less than that of } c_{i, e - I} V_1^p + \text{a polynomial whose } Y\text{-degree is strictly less than } p(e - I).$$

(11.10)

Let $w'$ denote a monomial of maximum $V_1$-degree which appears in $c_{i, e - I} V_1^p(YU_2)^{p(e - I)}$. Statements (11.8) and (11.9), together with the definitions of $e$ and $I$, imply that if $i \neq I$ or $j \neq e - I$, then $w'Y^{p(e - I)}$ does not divide any monomial which appears in $f^*(i, j)$. Equation (11.10) implies that the monomial $w'Y^{p(e - I)}$ appears in $f^*(I, e - I)$ and, for every integer $d > p(e - I)$, $w'Y^d$ does not appear in $f^*(I, e - I)$. These observations and Eq. (11.7) imply that

the monomial $w'Y^{p(e - I)}$ appears in $f^*$ and, for every integer $d > p(e - I)$, $w'Y^d$ does not appear in $f^*$.

(11.11)

One can write

$$f^* = \sum_w w f_w(Y), \text{ where the sum ranges over all monomials } w \text{ in } K[U_1, U_2, V_1, V_2] \text{ whose degrees are less than or equal to } \deg f \text{ and } f_w(Y) \in K[Y] \text{ for every } w.$$  

(11.12)

Note that if $Y$ is replaced by an element of $A$, then $f^* - f$ becomes zero,
because $f$ is an invariant of $\text{UT}(A)$. Therefore $f^* - f$ is divisible by $\prod_{a \in A} Y - a$. This observation and Eq. (11.12) imply that $f_w(Y) - f_w(0)$ is divisible by $\prod_{a \in A} Y - a$ for every monomial $w$. Note also that, by statements (11.6) and (11.11), the degree of $f_w(Y)$ is strictly less than $|A|$. Therefore $f_w(Y) - f_w(0)$ is identically zero, so $f_w(Y) \in K$. This inclusion and statements (11.11) and (11.12) imply that $p(e - I) - \deg f_w(Y) = 0$, so $e = I$. This observation and the second part of statement (11.6) imply that $p < |A|$. Since $p < |A|$, Eq. (11.5) and the definition of $e$ imply that $f$ lies in the $K[U_1, U_2, U, V_2 - U_2 V,]$-module generated by the monomials $V_1^e V_2^e$ such that $e_1 + e_2 < |A|$. Recall also that $f$ is an invariant of $\text{UT}(A)$; therefore Proposition 9 implies that $f \in K[U_1, U_2, U, V_2 - U_2 V,]$. This proves that $B_{\text{UT}(A)}$ is a subset of $K[U_1, U_2, U, V_2 - U_2 V,]$ ] This observation and Proposition 1 imply that $K[U_1, V_i, U_1 V_j - U_2 V_i : i = 1, 2]$. This observation and statement (11.2) establish the proposition. 

Remark. Proposition 8 implies that, if $|A| > 1$ and $m \geq 3$, then $K[U_1, V_i : 1 \leq i \leq m]^\text{UT}(A)$ does not equal $K[U_1, N_A(V_i), U_i V_j - U_j V_i : 1 \leq i, j \leq m]$.

5. SOME EXAMPLES OF INVARIANTS

If $G$ denotes a finite group of automorphisms of a commutative ring, then $\sum_{g \in G} r^s$ and $\prod_{g \in G} r^s$ are invariants of $G$ for every element $r$ in the ring. The next proposition describes other examples of invariants of $G$ in the case that $G = \text{UT}(A)$.

Notation. If $A'$ is a finite additive subgroup of $K$ and $f \in K[U_i, V_i : 1 \leq i \leq m]$, define $N_{A'}(f) = \prod_{\sigma \in \text{UT}(A')} f^\sigma$.

**Proposition 12.** Assume that $|A| > 1$. Let $A'$ denote a proper subgroup of $A$ and let $C$ denote a system of representatives for the cosets of $A'$ in $A$. Define

$$h = \sum_{c \in C} N_{A'}(V_1 + c U_1) N_{A'}(V_2 + c U_2) \cdots N_{A'}(V_m + c U_m)$$

and let $i^* = |A| / |A'|$. Then $h$ is an invariant of $\text{UT}(A)$ and, if $m \geq i^*$, then the monomial $(U_1 U_2 \cdots U_r - 1)^{i^* - 1} \prod_{i=m,i^*} V_i^{i^*}$ appears in $h$.

**Proof.** Let $\sigma(x)$ be defined as in the introduction and define

$$H(x) = \prod_{i=1}^m N_A(V_i + x U_i)$$
for every \( x \in K \). Note that
\[
H(x)^{a(x)} = H(x + y) \quad \text{for all } x, y \in K. \tag{12.1}
\]

Observe that \( N_{A'}(V_i + xU_i + a'U_i) = N_{A'}(V_i + xU_i) \) for every \( x \in K, a' \in A', \) and \( i \in \{1, \ldots, m\} \). Therefore \( h \) does not depend on the choice of the system of representatives \( C \) for the cosets of \( A' \). Observe that, if \( a \in A \), then
\[
h = \sum_{c \in C} H(c + a), \quad \text{because } \{c + a : c \in C\} \text{ is a system of representatives for the cosets of } A' \text{ in } A
\]

\[
= \sum_{c \in C} H(c)^{a(a)}, \quad \text{by (12.1)}
\]

\[
= h^{a(a)}.
\]

This proves that \( h \) is an invariant of \( UT(A) \).

Suppose that \( m \geq i^* \) and \( c \in C \). Note that, for \( i = 1, 2, \ldots, m \),
\[
N_{A'}(V_i + cU_i) = V_i^{[A']} + \text{an element of } U_iK[U_i, V_i]
\]

and
\[
N_{A'}(V_i + cU_i) = \left( \prod_{a \in A'} c + a \right) U_i^{[A']} + \text{an element of } V_iK[U_i, V_i]
\]

\[
= \left( \prod_{a \in A'} c - a \right) U_i^{[A']} + \text{an element of } V_iK[U_i, V_i]
\]

because the map \( a \mapsto -a \) permutes the elements of \( A' \).

Therefore
\[
\text{the coefficient of } (U_1U_2 \cdots U_{i^*})^{[A']} \prod_{j=i^*}^{m} V_j^{[A']} \text{ in } H(c)
\]

\[
is \prod_{a \in A'} (c - a)^{i^* - 1} \tag{12.2}
\]

Define \( f_{A'}(X) = \prod_{a \in A'} X - a \). The theory of \( p \)-polynomials [13, pp. 564–565] implies that
\[
f_{A'}(x + y) = f_{A'}(x) + f_{A'}(y) \quad \text{for all } x, y \in K. \tag{12.3}
\]

Therefore the restriction of \( f_{A'} \) to \( A \) gives a homomorphism between the additive groups \( A \) and \( f_{A'}(A) \). Note also that the kernel of this homomorphism is \( A' \), so \( |f_{A'}(A)| = |A|/|A'| = i^* \). This observation and Proposition 7 imply that

\[
\sum_{x \in f_{A'}(A)} x^{i^* - 1} \neq 0. \tag{12.4}
\]
Note that

\[
\text{the coefficient of } (U_1 U_2 \cdots U_{i-1})^{A_1} \prod_{i=1}^{m} V_i^{A_i} \text{ in } h = \sum_{c \in C} f_{A'}(c)^{i^* - 1}, \quad \text{by (12.2)}
\]

\[
= \sum_{x \in f_{A'}(C)} x^{i^* - 1}, \quad \text{because the map } c \mapsto f_{A'}(c)
\]

gives a one-to-one correspondence between \( C \)
and \( f_{A'}(A) \)

\[ \neq 0, \quad \text{by (12.4)}. \]

This establishes the last assertion of the proposition. \( \square \)

Remarks. Let \( h \) be defined as in Proposition 12.

1. The following argument shows that the \( U \)-degree of every monomial which appears in \( h \) is greater than or equal to \(|A| - |A'|\). Equation (12.3) (with \( K \) replaced by \( K(U_i, V_i; 1 \leq i \leq m) \)) and the fact that \( N_A(V_i + cU_i) = U_i^{A_1'} f_{A'}((V_i/U_i) + c) \) imply that \( N_A(V_i + cU_i) = N_A(V_i) + f_{A'}(c) U_i^{A_1'} \) for every \( i \in \{1, \ldots, m\} \) and \( c \in K \). This observation and the definition of \( h \) imply that

\[
h = \sum_{c \in C} (N_A(V_1) + f_{A'}(c) U_1^{A_1'}) \cdots (N_A(V_m) + f_{A'}(c) U_m^{A_m'}). \tag{12.5}
\]

The proof of Proposition 12 shows that \( f_{A'}(A) \) is an additive group of size \( i^* \). Therefore the first equation of statement (7.6) (with \( A \) replaced by \( f_{A'}(A) \)) implies that

\[
\sum_{x \in f_{A'}(A)} x^j = 0 \quad \text{when } 1 \leq j < i^* - 1.
\]

This observation and the fact that the map \( c \mapsto f_{A'}(c) \) gives a one-to-one correspondence between \( C \) and \( f_{A'}(A) \) imply that

\[
\sum_{c \in C} f_{A'}(c)^j = 0 \quad \text{when } 1 \leq j < i^* - 1. \tag{12.6}
\]

Note also that

\[
|C| \text{ is divisible by } p, \tag{12.7}
\]

because \(|C| = |A|/|A'|\), \( A' \) is a proper subgroup of \( A \), and \( A \) is a vector space over \( F_p \). Statements (12.5)–(12.7) imply that \( h \) is a linear combination of polynomials of the form

\[
\left( \prod_{i \in S} U_i^{A_i} \right) \left( \prod_{i \in \{1, \ldots, m\} - S} N_A(V_i) \right),
\]
where \( S \) denotes a subset of \( \{1, \ldots, m\} \) whose size is greater than or equal to \( i^* - 1 \). Therefore the \( U \)-degree of every monomial which appears in \( h \) is greater than or equal to \( |A'|-1 = |A| - |A'| \).

2. The following argument shows that, if \( |A'| > 1 \) and \( m \geq i^* \), then \( h \) does not lie in \( \{\sum_{\sigma \in UT(A)} f^\sigma \mid N_A(f) \in K[U_i, V_i \mid 1 \leq i \leq m] \} \). The first equation of statement (7.6) implies that

\[
\text{if } 1 \leq j < |A| - 1, \text{ then } \sum_{a \in A} a^j = 0. \tag{12.8}
\]

Let \( w \) denote the monomial \( V_1^{e_1}V_2^{e_2} \cdots V_m^{e_m} \) and observe that

\[
\sum_{\sigma \in UT(A)} w^\sigma = \sum_{a \in A} (V_1 + aU_1)^{e_1} (V_2 + aU_2)^{e_2} \cdots (V_m + aU_m)^{e_m}.
\]

This equation, statement (12.8), and the fact that \( |A| \) is divisible by \( p \) imply that the \( U \)-degree of every monomial which appears in \( \sum_{\sigma \in UT(A)} w^\sigma \) is greater than or equal to \( |A| - 1 \). This observation and the fact that \( K[U_i, V_i \mid 1 \leq i \leq m] \) is generated as a \( K[U_i, \ldots, U_m] \)-module by monomials of the form \( V_1^{e_1} \cdots V_m^{e_m} \) imply that

\[
\text{if } f \in K[U_i, V_i \mid 1 \leq i \leq m], \text{ then the } U \text{-degree of every monomial which appears in } \sum_{\sigma \in UT(A)} f^\sigma \text{ is greater than or equal to } |A| - 1. \tag{12.9}
\]

Assume that \( m \geq i^* \). Proposition 12 and statement (12.9) imply that, if \( |A'| > 1 \), then \( h \) does not lie in the \( K \)-algebra generated by \( \{\sum_{\sigma \in UT(A)} f^\sigma \mid f \in K[U_i, V_i \mid 1 \leq i \leq m] \} \).

Suppose that \( f \in K[U_i, V_i \mid 1 \leq i \leq m] \). If the \( U \)-degree of every monomial which appears in \( f \) is strictly greater than 0, then the \( U \)-degree of every monomial which appears in \( N_A(f) \) is greater than or equal to \( |A| \). This observation and Proposition 12 imply that, if the \( U \)-degree of every monomial which appears in \( f \) is strictly greater than 0, then \( N_A(f) \neq h \). If there is a monomial of \( U \)-degree 0 which appears in \( f \), then there is a monomial of \( U \)-degree 0 which appears in \( N_A(f) \). This observation and Remark 1 imply that, if there is a monomial of \( U \)-degree 0 which appears in \( f \), then \( N_A(f) \neq h \). Thus \( N_A(f) \neq h \) for all \( f \).

3. Assume that \( |A| > 1 \) and let \( b \) denote a strictly positive integer such that \( p^b \leq |A| \). The following examples show that the lower bound for \( d_1 + \cdots + d_m \) given in Proposition 5 is attained in infinitely many cases. Define \( i^* = |A|/p^{b-1} \) and set

\[
w(m) = (U_1 U_2 \cdots U_{i^* - 1}) p^{b-1} \prod_{i = i^*}^m V_i^{p^{b-1}} \quad \text{if } m > i^*
\]
and
\[ w(m) = (U_i^{m-1}V_2V_3\cdots V_m)^{p^b-1} \quad \text{if} \quad 2 \leq m \leq i^*. \]

Since \( A \) is a vector space over \( F_p \) and \( |A| \geq p^b \geq p \), there is a subgroup \( A' \) of \( A \) such that \( |A'| = p^b - 1 \). This observation and Proposition 12 imply that if \( m > i^* \), then the monomial \( w(m) \) appears in an invariant of \( UT(A) \). If \( 2 \leq m \leq i^* \), then the monomial \( w(m) \) appears in \( \prod_{i=2}^{m} (U_iV_i - U_iV_i')^p \), which is an invariant of \( UT(A) \).

If \( 2 \leq m \leq i^* \), then \( (m - 1) p^b - 1 \leq (i^* - 1) p^b - 1 = |A| - p^b - 1 \) and
\[ U\text{-degree} \ w(m) = V\text{-degree} \ w(m) \leq |A| - p^b - 1. \]

If \( m \geq \max\{2i^* - 2, \ i^* + 1\} \), then \( (m - i^* + 1) p^b - 1 \geq (i^* - 1) p^b - 1 = U\text{-degree} \ w(m) \), so
\[ U\text{-degree} \ w(m) = |A| - p^b - 1 \leq (m - i^* + 1) p^b - 1 = V\text{-degree} \ w(m). \]

These observations imply that if \( 2 \leq m \leq i^* \) or \( m \geq 2i^* - 2 \), then the monomial \( w(m) \) satisfies the hypotheses on \( \prod_i U_i^{d_i}V_i \), stated in Proposition 5 and the corresponding bound for \( d_1 + \cdots + d_m \) is attained.

4. The following example shows that the degree hypothesis in Proposition 10 cannot be weakened when \( |A| > 1 \) and \( m \geq 2p - 1 \). Assume that \( |A| > 1 \) and let \( w = (U_1U_2\cdots U_{p-1})^{(|A|/p)\cdot \prod_{i=2}^{p-1} V_i^{A_i/p}}. \) Define \( B_m \) as in Proposition 1 and note that \( w \in B_m \). Note also that \( U\text{-degree} \ w = |A| - |A|/p < (\deg w)/2 \); therefore
\[ w \text{ does not appear in an element of } [U_i, N_A(V_i), U_iV_j - U_jV_i : 1 \leq i, j \leq m]. \tag{12.10} \]

Let \( A' \) denote a subgroup of \( A \) of size \( |A|/p \); such a subgroup exists because \( A \) is a vector space over \( F_p \) and \( |A| > 1 \). Define \( h \) as in Proposition 12, with \( m = 2p - 1 \). Proposition 12 implies that \( w \) appears in \( h \); this observation and statement (12.10) imply that \( h \) does not lie in \( K[U_i, N_A(V_i), U_iV_j - U_jV_i : 1 \leq i, j \leq m] \). Proposition 12 also implies that \( h \) is an invariant of \( UT(A) \). Thus, if \( m \geq 2p - 1 \), then \( K[U_i, V_i : 1 \leq i \leq m]^{UT(A)} \) contains a polynomial of degree \( 2|A| - |A|/p \) (namely \( h \)) which does not lie in \( K[U_i, N_A(V_i), U_iV_j - U_jV_i : 1 \leq i, j \leq m] \).

Recall from the introduction that \( \{C_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\} \) denotes a set of commuting indeterminates.
**Proposition 13.** Let $F$ denote a finite field and let $b$, $m$, and $n$ denote positive integers. Let

$$h = \sum_{(t_1, \ldots, t_n) \in F^n} \prod_{i=1}^m (t_1 C_{i1} + t_2 C_{i2} + \cdots + t_n C_{im})^b.$$ 

Then $h$ is a vector invariant of $GL(n, F)$, i.e., $h^g = h$ for every $g \in GL(n, F)$.

Let $d$ denote a positive integer such that $bd$ is divisible by $|F| - 1$, and assume that $m \geq nd$ and $bm$ is divisible by $|F| - 1$. Define

$$w = \left(\prod_{j=1}^{n-1} \prod_{k=1}^d C_{jd} - d + k \right) \left( \prod_{k=\{n-1\}d+1}^m K C_{kn} \right);$$

then the coefficient of $w^b$ in $h$ is $(-1)^n$.

**Proof.** Let $L = FC_{11} + FC_{12} + \cdots + FC_{1n}$. If $i \in \{1, \ldots, m\}$, let $H_i$ denote the $K$-algebra homomorphism from $K[C_{ij} : 1 \leq j < n]$ to $K[C_{ij} : 1 \leq j \leq n]$ such that $H_i(C_{ij}) = C_{ij}$ for $j = 1, \ldots, n$. Suppose that $g \in GL(n, F)$ and observe that

$$h = \sum_{x \in L} (H_1(x))^b (H_2(x))^b \cdots (H_m(x))^b = \sum_{x \in L} (H_1(x^g))^b (H_2(x^g))^b \cdots (H_m(x^g))^b$$

because the map $x \mapsto x^g$ permutes the elements of $L$

$$= h^g,$$  because $H_i(x^g) = H_i(x)^g$ for every $i$ and $x$.

This establishes the first assertion of the proposition.

Assume now that $m \geq nd$ and $bm$ is divisible by $|F| - 1$. The definitions of $h$ and $w$ imply that

the coefficient of $w^b$ in $h$

$$= \sum_{(t_1, \ldots, t_n) \in F^n} \left(\prod_{j=1}^{n-1} t_j^{bd} \right) t_n^{(m - nd + d)h}$$

$$= \left(\sum_{t_1 \in F} t_1^{bd} \right) \left(\sum_{t_2 \in F} t_2^{bd} \right) \cdots \left(\sum_{t_{n-1} \in F} t_{n-1}^{bd} \right) \left(\sum_{t_n \in F} t_n^{(m - nd + d)h} \right)$$

$$= (|F| - 1)^n,$$  by Eq. (7.11) and the fact that $bd$ and $bm$ are divisible by $|F| - 1$

$$= (-1)^n,$$  because $|F|$ is a multiple of the characteristic of $F$.  ■
6. Vector Invariants over Finite Fields

Let \( I \) denote the identity matrix.

**Proposition 14.** Let \( F \) denote a finite subfield of \( K \) and let \( G \) denote a subgroup of \( \text{GL}(n, F) \). Assume that there is an element \( g \) in \( G \) such that \((g - I)^2 = 0\) and \( \text{rank}(g - I) = 1 \). Let \( A \) denote the set of elements \( x \) in \( F \) such that \( I + x(g - I) \in G \). Let \( d \) denote the smallest integer such that \( d > 0 \) and \( (|A| - 1)d \) is divisible by \( |F| - 1 \). If \( m \geq (n + 1)d \), then every set of \( K \)-algebra generators of \( K[C_{ij}: 1 \leq i \leq m, 1 \leq j \leq n]_G \) contains a generator whose degree is greater than or equal to \((\lfloor m/d \rfloor - n + 2)(|A| - 1)/p\); here \( \lfloor \cdot \rfloor \) denotes the greatest-integer function.

**Proof.** If \( n \geq 2 \), let \( E_{n-1,n} \) denote the \( n \times n \) matrix whose \((n-1, n)\)th entry is 1 and whose other entries are zeros. The assumptions about \( g \) imply that \( n \geq 2 \) and \( g \) is similar to \( I + E_{n-1,n} \). Therefore, after a linear change of coordinates, one may assume that

\[
C_{i1}, C_{i2}, \ldots, C_{in-1} \text{ are each fixed by } g \quad \text{and} \quad C_{in}^g = C_{in} \quad \text{for every } i.
\]

(14.1)

Let \( m' \) denote the biggest integer such that \( m' \leq m \) and \( m' \) is divisible by \( d \). Suppose that \( m \geq (n+1)d \); then \( m' \geq (n+1)d \). Define

\[
w = \left( \prod_{j=1}^{n-1} \prod_{k=0}^{d} C_{j, d}, \ldots, C_{i, n-1} \right) \left( \prod_{k=(n-1)d+1}^{m'} C_{kn} \right).
\]

Proposition 13 (with \( m \) and \( b \) replaced by \( m' \) and \( |A| - 1 \), respectively) implies that the monomial \( w^{(|A| - 1)} \) appears in an invariant of \( G \). Let \( S(m) \) denote a set of \( K \)-algebra generators of \( K[C_{ij}: 1 \leq i \leq m, 1 \leq j \leq n]_G \). Note that \( w^{(|A| - 1)} \) appears in an element of the \( K \)-algebra generated by \( S(m) \), so one can write

\[
w^{(|A| - 1)} = w_1 w_2 \cdots w_r, \quad \text{where each } w_i \text{ is a non-constant monomial which appears in an element of } S(m).
\]

(14.2)

If \( x \) and \( y \) denote elements of \( A \), then

\[
I + (x + y)(g - I) = (I + x(g - I))(I + y(g - I)), \quad \text{because } (g - I)^2 = 0
\]

\[\in G, \quad \text{because } I + x(g - I) \text{ and } I + y(g - I) \text{ both lie in } G \text{ and } G \text{ is a group.}
\]

Therefore \( A \) is closed under addition and \( \{I + x(g - I) : x \in A\} \) is a subgroup of \( G \). Define the \( U \)-degree of a monomial \( \prod_{i=1}^n \prod_{j=1}^m C_{ij}^{c_{ij}} \) to be
e(1, n - 1) + e(2, n - 1) + \ldots + e(m, n - 1) and define its $V$-degree to be $e(1, n) + e(2, n) + \ldots + e(m, n)$. Let $w_1, w_2, \ldots, w_t$ be as in Eq. (14.2). Condition (14.1) implies that the group $\{1 + x(g - I) : x \in A\}$ can be identified with $UT(A)$ (where the indeterminates $U_i$ and $V_i$ correspond to $C_{i,n-1}$ and $C_{m,i}$, respectively, for every $i$). Therefore Proposition 5, with $p^b = |A|$, implies that

$$U\text{-degree } w_i \geq \min\{|A| - |A|/p, V\text{-degree } w_i\} \quad \text{for every } i. \quad (14.3)$$

This inequality implies that

if $U\text{-degree } w_i + V\text{-degree } w_i > 0$, then $U\text{-degree } w_i > 0. \quad (14.4)$

Equation (14.2) implies that there is a number $J$ in $\{1, \ldots, t\}$ such that $U\text{-degree } w_J + V\text{-degree } w_J > 0$ and

$$U\text{-degree } w_J/(U\text{-degree } w_J + V\text{-degree } w_J) \leq U\text{-degree } w^{[d]}/(U\text{-degree } w^{[d]} + V\text{-degree } w^{[d]}) = d/(m' - (n - 2)d). \quad (14.5)$$

This relation and the fact that $m' \geq (n + 1)d$ imply that $U\text{-degree } w_J/(U\text{-degree } w_J + V\text{-degree } w_J) \leq \frac{1}{2}$; hence $2(U\text{-degree } w_J) \leq V\text{-degree } w_J$. This inequality and statement (14.4) (with $i$ replaced by $J$) imply that $U\text{-degree } w_J > V\text{-degree } w_J$. This inequality and statement (14.3) imply that $U\text{-degree } w_J \geq |A| - |A|/p$. Observe that

$$\deg w_J \geq U\text{-degree } w_J + V\text{-degree } w_J \geq (m' - (n - 2)d)(|A| - |A|/p)/d, \quad \text{by (14.5) and the fact that } U\text{-degree } w_J \geq |A| - |A|/p$$

$$= ([m/d] - n + 2)(|A| - |A|/p), \quad \text{because } m'/d = [m/d].$$

This observation and the fact that $w_J$ appears in some element of $S(m)$ imply that the degree of some element of $S(m)$ is greater than or equal to $([m/d] - n + 2)(|A| - |A|/p)$. \hfill \Box

**Proposition 15.** Let $F$, $G$, and $g$ be as in Proposition 14. Assume that $I + x(g - I) \in G$ for every $x \in F$. If $m \geq n + 1$, then every set of $K$-algebra generators of $K[C_{ij} : 1 \leq i \leq m, 1 \leq j \leq m]_G$ contains a generator whose degree is greater than or equal to $(m - n + 2)(|F| - 1)$.

**Proof.** Assume that $m \geq n + 1$ and define $w$ (with $d = 1$) and $S(m)$ as in the proof of Proposition 14. Note that the conditions of Proposition 14 are
satisfied with $A = F$ and $d = 1$; therefore the statements derived in the proof of Proposition 14 are valid here.

Let $K' = K(C_i : 1 \leq i \leq m, 1 \leq j \leq n - 2)$ and let $U_i = C_{i,n}$ and $V_i = C_{i,n}$ for every $i$. Condition (14.1) and the hypothesis that $I + x(g - I) \in G$ for every $x \in F$ imply that the invariants of $G$ are also invariants of $UT(F)$ (here $UT(F)$ is a group of automorphisms of $K'[U_i, V_i : 1 \leq i \leq m]$). Therefore

$$S(m) \text{ is a set of invariants of } UT(F). \quad (15.1)$$

Note that the monomial $w^{[F]-1}$ appears in an invariant of $G$ (by Proposition 13), so it appears in an element of $K[s : s \in S(m)]$. Note also that

$$w^{[F]-1}/(C_{1,1} C_{2,1} \cdots C_{n-2,n-2})^{[F]-1} = (U_{n-1} V_n V_{n+1} \cdots V_m)^{[F]-1}. \quad (15.1)$$

Therefore $(U_{n-1} V_n V_{n+1} \cdots V_m)^{[F]-1}$ appears in an element of the $K'$-subalgebra of $K'[U_i, V_i : 1 \leq i \leq m]$ generated by $S(m)$. Since $(U_{n-1} V_n V_{n+1} \cdots V_m)^{[F]-1}$ appears in an element of this subalgebra, statement (15.1) and Proposition 6 (with an appropriate relabelling of the subscripts of $U_1, ..., U_m, V_1, ..., V_m$) imply that it also appears in an element of $S(m)$. Let $s^*$ denote an element of $S(m)$ in which $(U_{n-1} V_n V_{n+1} \cdots V_m)^{[F]-1}$ appears. Note that

$$\deg s^* \geq \deg (U_{n-1} V_n V_{n+1} \cdots V_m)^{[F]-1},$$

because $(U_{n-1} V_n V_{n+1} \cdots V_m)^{[F]-1}$ appears in $s^*$

$$= (m - n + 2)([F]-1).$$

This establishes the proposition. 

ACKNOWLEDGMENT

I am grateful to Professor Ian Hughes for telling me about his work with Campbell and Pollack [1] and encouraging me to investigate the invariants of $UT(F_p)$.

REFERENCES


