VECTOR INVARIANTS OF $\text{Syl}_p(\text{GL}(n, \mathbb{F}_q))$ AND THEIR HILBERT IDEALS

CHRIS MONICO AND MARA D. NEUSEL

Abstract. We describe the Hilbert ideal of the vector invariants of a $p$-Sylow subgroup of the general linear group.

1. Introduction

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of characteristic $p$ and order $q = p^s$. Consider the general linear group of $d \times d$ matrices over this field, $\text{GL}(d, \mathbb{F})$.

The group $\text{GL}(d, \mathbb{F})$ acts on the vector space $W = \mathbb{F}^d$ by matrix multiplication, which induces an action on the dual space and hence on the full symmetric algebra on the dual, denoted by $\mathbb{F}[W]$. Its ring of polynomial invariants is the Dickson algebra, denoted by $D(d) = \mathbb{F}[W]^{\text{GL}(d, \mathbb{F})}$. Moreover for any subgroup $G \subseteq \text{GL}(d, \mathbb{F})$ we obtain

$$D(d) \hookrightarrow \mathbb{F}[W]^G \hookrightarrow \mathbb{F}[W]$$

a chain of Noetherian commutative $\mathbb{F}$-algebras, see [7] for more background on invariant theory of finite groups.

Consider a finite group $P$ and a faithful representation $\rho_1 : P \hookrightarrow \text{GL}(d, \mathbb{F})$ afforded by the upper triangular matrices

$$M = \begin{bmatrix} 1 & * \\ \vdots & \ddots \\ 0 & 1 \end{bmatrix} \in \text{GL}(d, \mathbb{F}).$$

The group $\rho_1(P) \cong P$ is a $p$-Sylow subgroup of the general linear group. Denote by $x_1, \ldots, x_d$ the standard dual basis of $W^*$. Then its ring of invariants can be written as the polynomial algebra

$$\mathbb{F}[x_1, \ldots, x_d]^P = \mathbb{F}[c_{\text{top}}(x_1), \ldots, c_{\text{top}}(x_d)]$$

where $c_{\text{top}}(x_i)$ denotes the top orbit Chern class of the basis element $x_i$, i.e., the product of all linear forms in the set $\{gx_i | g \in \rho_1(P)\}$, see, e.g., Example 2 in Section 4.5 in [7].

Received by the editors August 2014.

2000 Mathematics Subject Classification. Primary 13A50, Secondary.

Key words and phrases. Invariant Theory of Finite Groups, $p$-Sylow Groups, Vector Invariants, Generating Set, Transfer Variety, Hilbert Ideal.

The second author thanks the Simons Foundation for partially supporting this research.

©0000 (copyright holder)
In this article we consider the $n$-fold vector invariants of $P$, i.e., we embed the group $P$ into $\mathsf{GL}(dn, \mathbb{F})$

$$
\rho_n : P \hookrightarrow \mathsf{GL}(dn, \mathbb{F})
$$

afforded by the block diagonal matrices

$$
\text{block}(M, \ldots, M) = 
\begin{bmatrix}
M & \cdots & 0 \\
0 & \ddots & 0 \\
0 & \cdots & M
\end{bmatrix}
$$

for all $M \in \rho_1(P)$. Denote by $V = W^{\otimes n}$ the corresponding $dn$-dimensional vector space. We denote the standard dual basis of $V^*$ by $x_{11},\ldots,x_{1d},x_{21},\ldots,x_{2d},\ldots,x_{nd}$.

Recall that the Hilbert ideal of the ring of invariants $\mathbb{F}[V]^P$ is defined as the ideal in the ambient ring of polynomials generated by all invariants of positive degree

$$
\mathcal{H}(\rho_n(P)) = (\mathbb{F}[V]^P)\mathbb{F}[V].
$$

In this paper we prove the following result:

**Theorem 1.1.** The Hilbert ideal $\mathcal{H}(\rho_n(P))$ is generated by the top orbit Chern classes of the basis elements $x_{ji}$, $j = 1,\ldots,n$ and $i = 1,\ldots,d$.

Indeed, in the case of $d = 2$, this result follows from the description of the ring of invariants:

**Theorem 1.2.** The ring of invariants $\mathbb{F}[V]^P$ is generated by

$$
c_{\text{top}}(x_{j1}) \quad j = 1,\ldots,n,
$$

and the elements in the ideal $I = (x_{12},\ldots,x_{n2})\mathbb{F}[V] \cap \mathbb{F}[V]^P$.


In the next section we choose a term order and prove some technical preliminary results. In Section 3 we prove Theorem 1.2 and deduce Theorem 1.1 for the case $d = 2$. This serves as an induction start. The induction is completed in Section 4 proving Theorem 1.1 in general. In Section 5 we explain the significance of the ideal $I$ of Theorem 1.2: It is the radical of the image of the transfer.

2. Choosing a Good Term Order

We denote the variables as $x_{11},\ldots,x_{1d},x_{21},\ldots,x_{2d},\ldots,x_{n1},\ldots,x_{nd}$ and order them as follows

$$
x_{11} > x_{21} > \cdots > x_{n1} > x_{12} > \cdots > x_{n2} > \cdots > x_{1d} > \cdots > x_{nd}.
$$

This induces a lexicographic term order on the elements of $\mathbb{F}[V]$. We denote by $\text{LT}(\cdot)$ the leading term of $\cdot$. The following results motivate this choice of order.
Lemma 2.1. Let \( m \in \mathbb{F}[x_{11}, \ldots, x_{nd}] \) be a monomial. Then
\[
\text{LT}(gm) = m \quad \forall g \in P.
\]
Moreover, \( gm = m + h \) for some \( h \in (x_{12}, \ldots, x_{n2}, \ldots, x_{1d}, \ldots, x_{nd})\mathbb{F}[V] \).

Proof. Let \( m = x_{11}^{\alpha_{11}} \cdots x_{nd}^{\alpha_{nd}} \). Let \( \rho_n(g) = \text{block}(M, \ldots, M) \) where
\[
M = \begin{bmatrix}
1 & a_{12} & \cdots & a_{1d} \\
& \ddots & \ddots & \vdots \\
& \vdots & \ddots & a_{d-1,d} \\
& & & 0 \\
\end{bmatrix} \in \rho_1(P)
\]
be an arbitrary element of \( \rho_n(P) \). Then
\[
gm = \prod_{j,i} (x_{ji} + a_{ij}x_{j,i+1} + \cdots + a_{id}x_{jd})^{\alpha_{ji}}.
\]
Expanding this expression gives the desired result. \( \square \)

Lemma 2.2. If \( f \in \mathbb{F}[V]^P \) has a term \( x_{11}^{\alpha_{11}}x_{21}^{\alpha_{21}} \cdots x_{n1}^{\alpha_{n1}} \), then \( \alpha_{j1} \) is divisible by \( q^{d-1} \) for all \( j = 1, \ldots, n \).

Proof. We prove this by induction on \( n \). If \( n = 1 \) we have an explicit description of the ring of invariants (see introduction) and we note that the top orbit Chern class
\[
c_{\text{top}}(x_{11}) = x_{11}^{q^{d-1}} + \text{other terms}
\]
is the only generator with a term \( x_{11}^{\alpha_{11}} \).

Next, let \( n > 1 \). We consider the term
\[
m = x_{11}^{\alpha_{11}}x_{21}^{\alpha_{21}} \cdots x_{n1}^{\alpha_{n1}}.
\]
In case that there is a \( j_0 \) such that \( \alpha_{j0} = 0 \) we obtain our desired statement by induction hypothesis. So assume that \( \alpha_{j1} \neq 0 \) for all \( j = 1, \ldots, n \). We sort the invariant \( f \) by monomials \( x_{n1}^{\alpha_{n1}} \cdots x_{nd}^{\alpha_{nd}} \) and obtain
\[
f = \sum_I f_I x_{n1}^{\alpha_{n1}} \cdots x_{nd}^{\alpha_{nd}}
\]
where the sum runs over \( d \)-tuples \( I = (\alpha_{n1}, \ldots, \alpha_{nd}) \). Note that
\[
f_I = f_I(x_{11}, \ldots, x_{1d}, \ldots, x_{n-1,1}, \ldots, x_{n-1,d}).
\]
Our monomial \( m \) appears in \( f_{I_0}x_{n1}^{\alpha_{n1}} \) for \( I_0 = (\alpha_{n1}, 0, \ldots, 0) \). By Lemma 2.1 \( x_{n1}^{\alpha_{n1}} \) cannot be a nontrivial translate of any monomial. Therefore, \( f_{I_0} \) has to be an invariant. In particular we can assume by induction that \( \alpha_{11}, \ldots, \alpha_{n-1,1} \) are divisible by \( q^{d-1} \).

Switching the roles of \( n \) and, say, \( n-1 \) in this argument allows us to conclude that all \( \alpha_{j1}, j = 1, \ldots, n \) are divisible by \( q^{d-1} \). \( \square \)
3. The case of $2 \times 2$-matrices

In this section we prove Theorem 1.1 for the case $d = 2$, which serves as an induction start as it will become apparent in Section 4. We note that the result of this section was proven in [1] for the cases $q = 2, 4, n = 2, 3$, in addition to the papers mentioned in the introduction.

Consider the $p$-Sylow subgroup of $\text{GL}(2, F)$ given as follows:

$$\rho_1 : P \hookrightarrow \text{GL}(2, F)$$

where

$$P \cong \rho_1(P) = \{ M \in \text{GL}(2, F) | M = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} | a \in F \} \subseteq \text{GL}(2, F).$$

It is an elementary abelian $p$-group of rank $s$. Its ring of invariants is given by

$$F[x, y]^P = F[x^q - xy^{q-1}, y]$$

where we chose the standard dual basis $x, y$ for $V^*$. Note that this is a polynomial algebra generated by the top orbit Chern classes of the basis elements:

$$c_{\text{top}}(x) = \prod_{g \in P} gx = x^q - xy^{q-1} \quad c_{\text{top}}(y) = y.$$ 

Next consider the 2-fold vector invariants of $P$, i.e., we look at the faithful representation of $P$

$$\rho_2 : P \hookrightarrow \text{GL}(4, F)$$

afforded by the block diagonal matrices

$$\begin{bmatrix} 1 & a & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where $a \in F$. Its ring of invariants is given by

$$F[x_1, y_1, x_2, y_2]_P^F = F[c_{\text{top}}(x_1), y_1, c_{\text{top}}(x_2), y_2, Q_{12}]/(r)$$

where

$$Q_{12} = x_1 y_2 - x_2 y_1$$

and

$$r = Q_{12}^q - c_{\text{top}}(x_1)y_2^q + c_{\text{top}}(x_2)y_1^q - Q_{12}y_1^{q-1}y_2^{q-1}$$

see [6]. Next consider the $n$-fold vector invariants of $P$:

$$P \cong \rho_n(P) = \{ \begin{bmatrix} 1 & a & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} | a \in F \} \subseteq \text{GL}(2n, F).$$

We denote the standard dual basis as $x_1, y_1, x_2, y_2, \ldots, x_n, y_n$ and note that by choice of our order we have

$$x_1 > x_2 > \cdots > x_n > y_1 > \cdots > y_n.$$ 

---

1 This article treats only the case where $q = p$. However, the proof works in the general case.
Theorem 3.1. The ring of invariants $F[V]^P$ is generated by
\[ c_{\text{top}}(x_j), j = 1, \ldots, n \]
and the elements in the ideal $I = (y_1, \ldots, y_n)F[V] \cap F[V]^P$.

Proof. Let $A$ be the $F$ algebra generated by $c_{\text{top}}(x_j), j = 1, \ldots, n$ and the elements in the ideal $(y_1, \ldots, y_n)F[V] \cap F[V]^P$. By construction $A$ is a subalgebra of the invariants $F[V]^P$.

Any invariant $f$ such that each of its terms is divisible by one of the $y_j$'s is in $I$.

Next, let $f \in F[V]^P$ be an invariant not in $I$. Then $f$ contains a term $x_1^{a_1} \cdots x_n^{a_n}$.

By Lemma 2.2 we have that all the $\alpha$'s are divisible by $q$. Set $\alpha_j = qk_j$, then
\[ f - c_{\text{top}}(x_1)^{k_1} \cdots c_{\text{top}}(x_n)^{k_n} \]
is an invariant such that the monomial $x_1^{a_1} \cdots x_n^{a_n}$ is replaced by an element of the ideal $(y_1, \ldots, y_n)F[V]$, because
\[ c_{\text{top}}(x_1)^{k_1} \cdots c_{\text{top}}(x_n)^{k_n} = \prod_{j=1}^{n} (x_j^q - x_j y_j^{-1})^{k_j} = \prod_{j=1}^{n} (x_j^{qk_j}) + h \]
where $h \in (y_1, \ldots, y_n)F[V]$. Successively we obtain an invariant in $(y_1, \ldots, y_n)F[V]$ and hence in $I$. \hfill \Box

Corollary 3.2. The Hilbert ideal is generated by the top orbit Chern classes of the basis elements $x_1, \ldots, x_n, y_1, \ldots, y_n$.

Proof. The Hilbert ideal is generated by all invariants of positive degree, i.e., it is generated by the orbit Chern classes $c_{\text{top}}(x_1), \ldots, c_{\text{top}}(x_n)$ and the elements in the ideal $(y_1, \ldots, y_n)F[V] \cap F[V]^P$. Since the $y_j$'s are top orbit Chern classes (and in particular invariant) we are done. \hfill \Box

4. The General Case $d > 2$

We start by proving a refinement of Lemma 2.2 for the general case.

Lemma 4.1. Let $f \in F[V]^P$ be an invariant with a term
\[ m = x_1^{a_{11}} \cdots x_n^{a_{nd}}. \]
Then there exists a pair $j_0, i_0$ such that $\alpha_{j_0 i_0} \geq q^{d-1}$.

Proof. We proceed by induction on $d$.

Let $d = 2$. If $x_{j_0 i_2}$ divides $m$ for some $j_0 = 1, \ldots, n$ we are done. Otherwise,
\[ m = x_1^{a_{11}} \cdots x_n^{a_{n1}} \]
and our result follows from Lemma 2.2. Thus let $d > 2$.

If
\[ m = x_1^{a_{11}} x_2^{a_{21}} \cdots x_{n1}^{a_{n1}} \]
then we know by Lemma 2.2 that all the $\alpha_{j_1}$'s are divisible by $q^{d-1}$ as desired.

So consider monomials
\[ m = x_1^{a_{11}} \cdots x_{nd}^{a_{nd}} \]
such that there exists an exponent $\alpha_{j_1i_1} \neq 0$ for $i_1 \in \{2, \ldots, d\}$ and some $j_1$.

The group $\rho_0(P)$ contains subgroups $P_{\ell}$ consisting of block diagonal matrices
\[ \text{block}(M, \ldots, M) \]
n times
with
\[
M = \begin{bmatrix}
1 & a_{1,2} & 0 & \cdots & a_{1,d-1} \\
1 & a_{2,3} & \ddots & \cdots & a_{2,d-1} \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
1 & 0 & \cdots & 0 & 1 \\
& & & & a_{d-1,d}
\end{bmatrix}
\]
i.e., the \( r \)th column and the \( r \)th row are zero except at the \( r, r \) spot where there is a 1. We note that for all \( r = 1, \ldots, d \) the group \( P_r \) is isomorphic to the \( p \)-Sylow subgroup of \( \text{GL}(d-1, \mathbb{F}) \). The inclusion of groups induces an embedding of the invariants of \( P \) into those of \( P_r \).

Let us consider the group \( P_1 \). Then \( f \) as well as \( x_{11}, x_{21}, \ldots, x_{n1} \) are invariant under \( P_1 \). Sorting by monomials in the \( x_{j1} \)'s we obtain
\[
f = \sum_I f_I x_{\alpha_{11}11} \cdots x_{\alpha_{n1}n1}
\]
where the sum runs over \( n \)-tuples \( I = (\alpha_{11}, \ldots, \alpha_{n1}) \). Note that the polynomials \( f_I \) are \( P_1 \)-invariant. Thus by induction hypothesis we can assume that in each of the monomials appearing in a \( f_I \) there exists a \( j_0 \in \{1, \ldots, n\} \) and an \( i_0 \in \{2, \ldots, d\} \) such that
\[
\alpha_{j_0 i_0} \geq \gamma^{d-i_0}
\]
unless \( f_I \in \mathbb{F} \).

We are ready to prove Theorem 1.1 in general.

**Theorem 4.2.** The Hilbert ideal is generated by the top orbit Chern classes of the basis elements \( x_{ij} \), \( i = 1, \ldots, n \) and \( j = 1, \ldots, d \).

**Proof.** By construction
\[
J = (c_{\text{top}}(x_{ji}), \forall i, j) \subseteq \mathfrak{S}(\rho_n(P)).
\]
To show the reverse inclusion, let \( F \in \mathfrak{S}(\rho_n(P)) \). Then
\[
F = \sum_{r=1}^{n} H_r f_r
\]
for some nontrivial \( P \)-invariants \( f_r \) and some \( H_r \in \mathbb{F}[V] \). We proceed by induction on term order. The smallest monomial in any degree \( \delta \) is \( x_{nd}^\delta \) which is invariant as well as in our proposed ideal \( J \). Let
\[
LT(F) = x_{11}^{\beta_{11}} \cdots x_{nd}^{\beta_{nd}} > x_{nd}^{\beta_{11}+\cdots+\beta_{nd}}.
\]
Without loss of generality we can assume that the leading term of \( F \) appears in \( H_1 f_1 \):
\[
x_{11}^{\beta_{11}} \cdots x_{nd}^{\beta_{nd}} = \gamma h_1 x_{11}^{\alpha_{11}} \cdots x_{nd}^{\alpha_{nd}}
\]
for some \( \gamma \in \mathbb{F}^\times \), and some terms \( h_1 \in H_1 \) and \( x_{11}^{\alpha_{11}} \cdots x_{nd}^{\alpha_{nd}} \) in \( f_1 \). By Lemma 4.1 there exist \( j_0 i_0 \) such that
\[
\beta_{j_0 i_0} \geq \alpha_{j_0 i_0} \geq \gamma^{d-i_0}.
\]
Thus

\[ F - e_{\text{top}}(j_{\text{top}}) \beta_{j_{\text{top}}} - q^{d-1} \prod_{j \neq j_{\text{top}}} x_{ji}^{j_{ji}} < F. \]

Since the top orbit Chern classes are in the Hilbert ideal, we find by induction on term order that the LHS is in \( J \). Furthermore, the top orbit Chern classes are in \( J \), and therefore \( F \in J \).

Observe that this result shows the following:
- The maximal degree of a generator of the Hilbert ideal is \( q^{d-1} \) which is far less that the order of \( P \).
- The Hilbert ideal does not characterize the group \( P \) as any group between \( \rho_n(P) \) and \( \rho(\times nP) \) has the same orbit Chern classes of the basis elements and hence the same Hilbert ideal, where the representation \( \rho : \times nP \to \text{GL}(dn, \mathbb{F}) \) is afforded by the matrices
  
  \[ \text{block}(I, \ldots, I, M, I, \ldots, I) \]

where \( I \in \text{GL}(d, \mathbb{F}) \) is the identity matrix, and \( M \in \rho_1(P) \) appears in block \( j \) for \( j = 1, \ldots, n \). We will show in [5] that this phenomenon (and indeed a more general statement) remains valid for large classes of groups and representations.

5. The Transfer Variety of \( P \)

Recall that the transfer is given by

\[ \text{Tr}^P : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^P, \ f \mapsto \sum_{g \in P} gf. \]

It is an \( \mathbb{F}[V]^P \)-module map and as such its image is an ideal in \( \mathbb{F}[V]^P \). We denote by \( \partial_g \) the twisted differential given by

\[ \partial_g = 1 - g : V^* \longrightarrow V^*, \]

for \( g \in P \). We denote

\[ I_g = (\text{Im}(\partial_g)) \subseteq \mathbb{F}[V]. \]

By work of M. Feshbach, see, e.g., Theorem 6.4.7 in [7], we know that

\[ \text{Rad} \left( \text{Im} \text{Tr}^P \right) = \bigcap_{g, |g| = p} (I_g \cap \mathbb{F}[V]^P) \subseteq \mathbb{F}[V]^P. \]

Furthermore, the height of the image of the transfer is

\[ \text{height} \left( \text{Im} \text{Tr}^P \right) = \dim_{\mathbb{F}}(V) - \max \{ \dim_{\mathbb{F}} V^g \mid |g| = p \}. \]

Apparently, an element \( g \in \rho_n(P) \) of order \( p \) whose fixed point set has maximal dimension is given by

\[ g_0 = \text{block}(M, \ldots, M), \]

where \( M \) is an identity matrix with an additional 1 in the \( 1, d \) spot. Thus the height of the image of the transfer is \( dn - (d-1)n = n \).
Furthermore, note that
\[ \text{Im}(\partial_{g_0}) = \text{span}_F \{ x_{1d}, \ldots, x_{nd} \} \]

Thus
\[ I_{g_0} = (x_{1d}, \ldots, x_{nd}) \subseteq F[V] \]
is a prime ideal of height \( n \). By the Krull relations it follows that \( I_{g_0} \cap F[V]^P \) is a minimal isolated prime ideal of \( \text{ImTr}^P \).

More generally we claim the following.

**Proposition 5.1.** The radical of the image of the transfer of \( P \) is given by
\[ \text{Rad}(\text{ImTr}^P) = \bigcap_a (l_{a,1}, \ldots, l_{a,n}) \cap F[V]^P \]
where \( a = (a_2, \ldots, a_d) \in F^{d-1} \setminus \{0\} \) and \( l_{a,j} = a_2x_{j2} + \cdots + a_nx_{jn} \).

**Proof.** We note that any element \( g_a = \text{block}(M, \ldots, M) \) where \( a = (a_2, \ldots, a_d) \in F^{d-1} \setminus \{0\} \) and
\[
M = \begin{bmatrix}
1 & a_2 & a_3 & \cdots & a_d \\
\vdots & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & 0 \\
\vdots & & & 1
\end{bmatrix}
\]
has order \( p \). The ideal \( I_{g_a} \) associated to this element is one of the ideals mentioned in the statement:
\[ I_{g_a} = (l_{a,1}, \ldots, l_{a,n}) \]
Finally, let \( g = \text{block}(M, \ldots, M) \) be an arbitrary element of order \( p \) and set
\[
M = \begin{bmatrix}
1 & a_{12} & \cdots & a_{1d} \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & a_{d-1,d} \\
\vdots & & & 1
\end{bmatrix}
\]
Then \( I_g \) is the ideal in \( F[V] \) generated by the linear forms
\[
a_{12}x_{j2} + \cdots + a_{1d}x_{jd}, \ldots, a_{d-1,d}x_{jd} \quad \forall j = 1, \ldots, n.
\]
However, \( I_g \supset I_{g_a} \) for \( a = (a_{12}, \ldots, a_{1d}) \).

Observe that for the case \( d = 2 \) we obtain
\[ \text{Rad}(\text{ImTr}^P) = (x_{12}, \ldots, x_{n2}) \cap F[V]^P \]
as the ideals \( I_g \) are equal for all \( g \in P \) of order \( p \), and hence the radical of the image of the transfer is prime of height \( n \). \( \square \)
References


Department of Mathematics and Statistics, MS 1042, Texas Tech University, Lubbock, Texas 79409
E-mail address: C.Monico@ttu.edu, Mara.D.Neusel@ttu.edu