The Invariant Rings of the Sylow groups of $GU(3,q^2)$, $GU(4,q^2)$, $Sp(4,q)$ and $O^+(4,q)$ in the natural characteristic

Jorge N. M. Ferreira [1]

Faculdade de Ciências Exatas e da Engenharia,
Universidade da Madeira
Campus Universitário da Penteada, 9020-105 Funchal
Portugal

Peter Fleischmann

School of Mathematics, Statistics and Actuarial Science,
University of Kent,
Canterbury, Kent CT2 7NF
United Kingdom

Abstract

Let G be a Sylow p-subgroup of the unitary groups $GU(3,q^2)$, $GU(4,q^2)$, the sympletic group $Sp(4,q)$ and, for q odd, the orthogonal group $O^+(4,q)$. In this paper we construct a presentation for the invariant ring of G acting on the natural module. In particular we prove that these rings are generated by orbit products of variables and certain invariant polynomials which are images under Steenrod operations, applied to the respective invariant form defining the corresponding classical group. We also show that these generators form a $SAGBI$ basis and the invariant ring for G is a complete intersection.

Key words: Invariant Rings; SAGBI bases; Modular Invariant Theory; Sylow Subgroups; Finite Classical Groups.

1. Introduction

Let $\mathbb{F}$ be a field, V a finite dimensional $\mathbb{F}$-vector space and G a finite subgroup of $\mathrm{GL}(V)$. Then G acts naturally on the symmetric algebra $S := \mathbb{F}[V] := \mathrm{Sym}(V^*)$, by graded algebra

[1] The author was supported by Fundação para a Ciência e Tecnologia, through Programa Operacional Potencial Humano (POPH) do Fundo Social Europeu (FSE), by the PhD grant SFRH/BD/30132/2006.

automorphisms. One of the main problems of invariant theory is the investigation of the structure of the *ring of invariants*

$$R := \mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \mid g \cdot f = f \ \forall\ g \in G\}.$$

Since G is finite it is easy to see that S is a finitely generated R-module, which implies, by a classical result of Emmy Noether, that R is a finitely generated $\mathbb{F}$-algebra. Moreover the extension of quotient fields $\mathbb{L} := \mathrm{Quot}(S) \geq \mathbb{K} := \mathrm{Quot}(R) = \mathbb{L}^G$ is finite Galois with group G and the ring R is a normal domain, i.e. R is integrally closed in $\mathbb{K}$.
There are several constructive procedures that, if applied to ring elements $f \in S$, transform them into invariants in R: two examples are the *transfer-* or *trace map* $f \mapsto \mathrm{tr}(f) = \sum_{g\in G} g \cdot f$ and the *norm* $f \mapsto \mathrm{Norm}(f) := \prod_{g\in G} g \cdot f$. In general, these operations will generate a subalgebra $A \leq R$ and the major open question remains, how to find a set of *generating invariants* of R as an $\mathbb{F}$-algebra.

There is a particularly useful structure, present in invariant theory over the finite field $\mathbb{F}_q$: Let $\mathfrak{F} := \mathbb{F}_q[V]$. Then the q - *Steenrod algebra* $\mathcal{A} := \mathcal{A}_q$ is the graded $\mathbb{F}_q$-subalgebra $\mathcal{A} = \mathbb{F}\langle \mathcal{P}^i \mid i \in \mathbb{N}_0\rangle \leq \mathrm{End}_{\mathbb{F}_q}(\mathfrak{F})$, generated by the homogeneous *Steenrod operators* $\mathcal{P}^i$ of degree $i(q-1)$, which themselves are uniquely determined as elements of $\mathrm{End}_{\mathbb{F}_q}(\mathfrak{F})$, by the following rules:

(i) $\mathcal{P}^0 = \mathrm{id}_{\mathfrak{F}}$;

(ii) the Cartan identity $\mathcal{P}^i(fg) = \sum_{\substack{0\leq r,s\\ r+s=i}} \mathcal{P}^r(f)\mathcal{P}^s(g)$;

(iii) $\mathcal{P}^1(x_j) = x_j^q$ and $\mathcal{P}^k(x_j) = 0,\ \forall k > 1, j \geq 1$.

The elements $\mathcal{P}^i$ are also uniquely determined by the requirement that

$$\mathcal{P}(\zeta) :\ \mathfrak{F} \to \mathfrak{F}[[\zeta]],\ f \mapsto \sum_{i\geq 0} \mathcal{P}^i(f)\zeta^i$$

is the unique homomorphism of $\mathbb{F}$ - algebras which maps v to $v+v^q\zeta$ for each $v \in \langle x_1, x_2, \ldots, x_n\rangle_{\mathbb{F}}$. From this it is easy to see that $\mathcal{A}$ acts on $\mathbb{F}_q[V]$, commuting with the natural action of $\mathrm{GL}(V)$. Therefore since $G \leq \mathrm{GL}(V)$, $\mathcal{A}$ also acts on $\mathbb{F}_q[V]^G$.

Now let X be any of the following finite classical groups:

- the general unitary groups $GU(3, q^2)$ and $GU(4, q^2)$ of dimension 3 and 4, defined over the field $\mathbb{F}_{q^2}$,
- the symplectic group $Sp(4, q)$ of dimension 4 over $\mathbb{F}_q$,
- the general orthogonal group $O^+(4, q)$ over $\mathbb{F}_q$, with q odd.

As usual X is defined as a subgroup of $\mathrm{GL}(V)$, fixing a certain form $h \in V^*$ or, in the case of unitary groups, a homogeneous element $h \in \mathbb{F}_{q^2}[V]$. In other words $X = \mathrm{Stab}_{\mathrm{GL}(V)}(h)$, hence for any subgroup $G \leq X$, automatically h is a G-invariant and so are the "Steenrod images" $\mathcal{P}^i(h)$. The explicit description of the ring of invariants of the groups $Sp(2m, q)$ (see Carlisle and Kropholler, 1992; Benson, 1993) and $GU(n, q^2)$ (see Huah and Shin-Yao, 2006) supports the conjecture that invariant rings of classical groups are always generated by "Dickson invariants" together with certain Steenrod images $\mathcal{P}^i(h)$ of the relevant form. Replacing Dickson invariants by "orbit products of variables" a similar conjecture can be made about the invariant rings of Sylow p-groups of X. This conjecture is also supported by MAGMA (Bosma et al., 1997) calculations and we show that this is the case for the groups considered here.

Let G be a Sylow p-subgroup of X. Then our main result can be stated in short form as follows:

Theorem 1. *Let $\mathbb{F}$ be a field containing the field of definition of X. The invariant ring $\mathbb{F}[V]^G$ is generated by G-orbit products of variables and Steenrod images of the form h defining X. Furthermore, these generators form a $SAGBI$ basis and $\mathbb{F}[V]^G$ is a complete intersection.*

When constructing the invariant ring it is usually an important first step to determine the invariant field. In the paper (Ferreira and Fleischmann, 2016), the authors have determined the generators for the invariant fields of Sylow p-subgroups for *all* finite classical groups in the natural characteristic. For the groups X, Theorems 4.10, 4.12, 4.14 and 4.16 in (Ferreira and Fleischmann, 2016) give:

Theorem 2. *Let G be a Sylow p-subgroup of X and h the form defining X. Then*

$$\mathbb{F}(V)^G = \mathbb{F}[x_1, N(x_2), \ldots, N(x_k), h],$$

$k = 2$ if $X = GU(3, q^2)$ and $k = 3$ if X is $GU(4, q^2)$, $Sp(4, q)$ or $O^+(4, q)$ with q odd.

The paper is organized as follows: in section 2 we recall some results about $SAGBI$ We will use the ideas in (Sturmfels, 1996) to prove Lemmas 11 and 12, which will play a crucial role in proving the main theorems of section 3.

Finally in section 3 we present the generators and their relations for the invariant rings for Sylow p-subgroups of $GU(3, q^2)$, $GU(4, q^2)$, $Sp(4, q)$ and $O^+(4, q)$ with q odd. It is known that for the Sylow p-subgroups of the general linear groups, the invariant rings are polynomial (see Campbell and Wehlau, 2011, Section 3.4). We will show that this is not true for the Sylow p-groups here under consideration. We will prove that their invariant rings are a complete intersection and that their generators form a $SAGBI$ basis.

Since the methods used are very similar, we only present the full details for the Sylow p-subgroup of $GU(3, q^2)$ and $GU(4, q^2)$. For the remaining ones, the details can be found in (Ferreira, 2011).

2. *SAGBI* Bases

The concept of SAGBI basis was first considered by Robbiano and Sweedler (1990) and by Kapur and Madlener (1989), separately. The acronym $SAGBI$ stands for "Subalgebra Analogs to Gröbner Bases for Ideals". Suppose that A is a subalgebra of $\mathbb{F}[x_1, \ldots, x_n]$ and that we have chosen some monomial ordering, $<$, on the monomials of $\mathbb{F}[x_1, \ldots, x_n]$. We write $LT(A)$ for the algebra generated by all leading monomials of non-zero elements of A.

Definition 3. A subset $C \subseteq A$ is a $SAGBI$ **Basis** of A if the algebra generated by the leading monomials of all the elements in C is equal to $LT(A)$.

Throughout the rest of this section, let $C := \{f_1, f_2, \ldots, f_m\}$ be a finite set of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ and A the $\mathbb{F}$-algebra generated by them. Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. The **subduction** of f over C is performed as follows:

(i) Set h:=f.

(ii) If h is a constant in $\mathbb{F}$ then stop, otherwise go to step (iii).

(iii) Check if there exist $c \in \mathbb{F}$ and exponents $u_1, u_2, \ldots, u_m \in \mathbb{N}$ such that $LT(h) := c \prod_{j=1}^{m} LT(f_j)^{u_j}$.

(iv) If step (iii) fails then stop, otherwise go to step (v).

(v) Replace h by $h - c \prod_{j=1}^{m} f_j^{u_j}$ and go to step (ii).

Note that each time we get to step (v), the polynomial $h - c\prod_{j=1}^{m} f_j^{u_j}$ will either be a constant or it will have a smaller leading monomial than $LM(h)$. This guarantees that the procedure will halt. If C is a $SAGBI$ basis for A and $f \in A$, then the subduction of f over C will end in a constant and therefore we can write f as a polynomial expression in $f_1, \ldots, f_m$. If $f \notin A$ then at some stage in the subduction process, step (iii) will fail. Hence, when C is a $SAGBI$ basis the subduction process can be used as an algebra membership test.

Definition 4. A tête-a-tête over $(f_1, \ldots, f_m)$ (where $f_i \in C$) is a pair $(\mathbf{u}, \mathbf{v})$, where $\mathbf{u}, \mathbf{v} \in \mathbb{N}^m$ such that

$$\prod_{i=1}^{m} LM(f_i)^{u_i} = \prod_{i=1}^{m} LM(f_i)^{v_i}.$$

Given a tête-a-tête, there is a non-zero constant $c \in \mathbb{F}$ such that the polynomial

$$S(\mathbf{u}, \mathbf{v}) := \prod_{i=1}^{m} f_i^{u_i} - c\prod_{i=1}^{m} f_i^{v_i}$$

is either a constant or has a smaller leading monomial.

Theorem 5. *The finite set C is a $SAGBI$ basis for A if and only if for each tête-a-tête $(\mathbf{u}, \mathbf{v})$, the subduction of $S(\mathbf{u}, \mathbf{v})$ over C terminates at an element of $\mathbb{F}$.*

Proof. See (Robbiano and Sweedler, 1990), Theorem 2.8. □

We present here another way to check whether C is a $SAGBI$ basis for A or not. For each f_i, with $i = 1, \ldots, m$, we associate its leading monomial with a vector $\mathbf{a_i} \in \mathbb{N}^n$ by

$$LM(f_i) = \prod_{j=1}^{n} x_j^{a_{ij}}.$$

Also, we define the algebra homomorphism

$$\phi : \mathbb{F}[t_1, t_2, \ldots, t_m] \longrightarrow \mathbb{F}[x_1, x_2, \ldots, x_n] \tag{1}$$

by $\phi(t_i) = \prod_{j=1}^{n} x_j^{a_{ij}}$ and the semigroup homomorphism

$$\pi : \mathbb{N}^m \longrightarrow \mathbb{N}^n$$

by $\pi(\mathbf{u}) = \pi(u_1, u_2, \ldots, u_m) = u_1\mathbf{a_1} + u_2\mathbf{a_2} + \cdots + u_m\mathbf{a_m}$.

Theorem 6. *Assume that $g_1, g_2, \ldots, g_s$ generate the kernel of ϕ as an ideal. Then C is a $SAGBI$ basis for A if and only if the subduction of $g_i(f_1, \ldots, f_m)$ terminates at a constant for all $i \in \{1, \ldots, s\}$.*

Proof. See Corollary 11.5 in (Sturmfels, 1996). □

Corollary 7. *Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ such that $LM(f_i) = x_i^{d_i}$ with d_i a non-negative integer. Then $\{f_1, \ldots, f_n\}$ is a $SAGBI$ basis for the algebra it generates.*

Proof. In this case the kernel of ϕ is trivial since $\phi(t_i) = x_i^{d_i}$. Applying Theorem 6 finishes the proof. □

The previous corollary can also be seen as a particular case of Proposition 5.2.2 in (Campbell and Wehlau, 2011).

In order to apply Theorem 6 we must be able to compute the generators for the kernel of ϕ. We shall write $\mathbf{T^u}$, $\mathbf{u} \in \mathbb{N}^m$, for the monomial $\prod_{j=1}^{m} t_j^{u_j}$.

Lemma 8. *The kernel of the homomorphism ϕ is spanned as a $\mathbb{F}$-vector space by the set of binomials*

$$\{\mathbf{T^u} - \mathbf{T^v} : \mathbf{u}, \mathbf{v} \in \mathbb{N}^m \text{ with } \pi(\mathbf{u}) = \pi(\mathbf{v})\}.$$

Proof. See Lemma 4.1 in (Sturmfels, 1996). □

Remark 9. The previous Lemma shows that kernel of ϕ is spanned by the binomials $\mathbf{T^u} - \mathbf{T^v}$ where $(\mathbf{u}, \mathbf{v})$ is a tête-a-tête.

For any tuple of integers $\mathbf{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m$, we let $\mathbf{u}^+ = (u_1^+, \ldots, u_m^+)$ and $\mathbf{u}^- = (u_1^-, \ldots, u_m^-)$ where $u_i^+ = \max\{u_i, 0\}$ and $u_i^- = \max\{-u_i, 0\}$. Hence we get $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-$. We shall write $\ker \pi$ for the set consisting of all vectors $\mathbf{u} \in \mathbb{Z}^m$ such that $\pi(\mathbf{u}^+) = \pi(\mathbf{u}^-)$.

Corollary 10. *The kernel of ϕ is spanned by the binomials*

$$\{\mathbf{T^{u^+}} - \mathbf{T^{u^-}} : \mathbf{u} \in \ker \pi\}.$$

Define a $n \times m$ matrix B whose columns are the vectors $\mathbf{a_i}$ corresponding to the leading monomials of the polynomials f_i. It is not hard to see that $\mathbf{u} \in \mathbb{Z}^m$ belongs to $\ker \pi$ if and only if $B\mathbf{u} = 0$. This means we should look for the solutions of the equation $B\mathbf{u} = 0$ which have integer coordinates. So let W be the real vector space formed by the solutions of $B\mathbf{u} = 0$. We shall only look at the cases when the dimension of W is 1 or 2. First, we assume that W has dimension 1:

Lemma 11. *Let $\mathbf{w} \in \mathbb{Z}^m$ be a basis for W such that $\alpha\mathbf{w} \in \mathbb{Z}^m$ if and only if $\alpha \in \mathbb{Z}$. Then the kernel of ϕ is generated as an ideal by the binomial $\mathbf{T^{w^+}} - \mathbf{T^{w^-}}$.*

Proof. According to Corollary 10, the result will follow if we can show that for any element $\mathbf{u} \in \ker \pi$ the binomial $\mathbf{T^{u^+}} - \mathbf{T^{u^-}}$ is an element in the ideal generated by $\mathbf{T^{w^+}} - \mathbf{T^{w^-}}$. So let $\mathbf{u} \in \ker \pi$. Then $\mathbf{u} \in W$ and we get $\mathbf{u} = \alpha\mathbf{w}$ with $\alpha \in \mathbb{Z}$. Without loss of generality we can assume that $\alpha > 0$. Hence $(\alpha\mathbf{w})^+ = \alpha\mathbf{w}^+$ and $(\alpha\mathbf{w})^- = \alpha\mathbf{w}^-$. If $\alpha = 1$, there is nothing to prove. For $\alpha > 1$ we get

$$\mathbf{T}^{(\alpha\mathbf{w})^+} - \mathbf{T}^{(\alpha\mathbf{w})^-} = \mathbf{T}^{\alpha\mathbf{w}^+} - \mathbf{T}^{\alpha\mathbf{w}^-} = (\mathbf{T^{w^+}} - \mathbf{T^{w^-}}) \sum_{j=0}^{\alpha-1} \mathbf{T}^{((\alpha-1)-j)\mathbf{w}^+ + j\mathbf{w}^-}$$

and therefore it belongs to ideal generated by $\mathbf{T^{w^+}} - \mathbf{T^{w^-}}$. □

Finally, we consider the case when the dimension of W is 2.

Lemma 12. *Assume that $\{\mathbf{w_1}, \mathbf{w_2}\} \subset \mathbb{Z}^m$ is a basis for W satisfying the following properties:*

(a) A linear combination $\alpha_1\mathbf{w_1} + \alpha_2\mathbf{w_2}$ belongs to $\mathbb{Z}^m$ if and only if $\alpha_1, \alpha_2 \in \mathbb{Z}$.

(b) For any vector $\mathbf{u} = \alpha_1\mathbf{w_1} + \alpha_2\mathbf{w_2} \in \mathbb{Z}^m$, one of the following holds:

(i) The vectors $\mathbf{u}^+ - (\alpha_1\mathbf{w_1})^+$ and $\mathbf{u}^- - (\alpha_2\mathbf{w_2})^-$ have non-negative entries.
(ii) The vectors $\mathbf{u}^+ - (\alpha_2\mathbf{w_2})^+$ and $\mathbf{u}^- - (\alpha_1\mathbf{w_1})^-$ have non-negative entries.

Then the kernel of ϕ is generated as an ideal by the binomials in the set

$$\mathcal{F} := \{\mathbf{T^{w_i^+}} - \mathbf{T^{w_i^-}} : i \in \{1, 2\}\}.$$

Proof. Just as in Lemma 11, it is enough to show that for any element $\mathbf{u} \in \ker \pi$ the binomial $\mathbf{T^{u^+}} - \mathbf{T^{u^-}}$ is an element in the ideal $< \mathcal{F} >$ generated by $\mathcal{F}$. Then, the result follows from

Corollary 10. Let $\mathbf{u} \in \ker \pi$. Then we can write $\mathbf{u} = \alpha_1 \mathbf{w_1} + \alpha_2 \mathbf{w_2}$ with $\{\mathbf{w_1}, \mathbf{w_2}\}$ satisfying **Hypothesis A**. For simplicity we write $\mathbf{u} = \mathbf{v_1} + \mathbf{v_2}$ with $\mathbf{v_1} = \alpha_1 \mathbf{w_1}$ and $\mathbf{v_2} = \alpha_2 \mathbf{w_2}$. Just as was done in the proof of Lemma 11 we can show that $\mathbf{T}^{\mathbf{v_1}^+} - \mathbf{T}^{\mathbf{v_1}^-}$ and $\mathbf{T}^{\mathbf{v_2}^+} - \mathbf{T}^{\mathbf{v_2}^-}$ belong to the ideal generated by $\mathbf{T}^{\mathbf{w_1}^+} - \mathbf{T}^{\mathbf{w_1}^-}$ and $\mathbf{T}^{\mathbf{w_2}^+} - \mathbf{T}^{\mathbf{w_2}^-}$, respectively. Hence $\mathbf{T}^{\mathbf{v_1}^+} - \mathbf{T}^{\mathbf{v_1}^-}$ and $\mathbf{T}^{\mathbf{v_2}^+} - \mathbf{T}^{\mathbf{v_2}^-}$ are elements in the ideal $< \mathcal{F} >$. Now, we shall prove that $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-} \in < \mathcal{F} >$. Note that from $\mathbf{u} = \mathbf{v_1} + \mathbf{v_2}$ we get $\mathbf{u}^+ + \mathbf{v_1}^- + \mathbf{v_2}^- = \mathbf{u}^- + \mathbf{v_1}^+ + \mathbf{v_2}^+$. If (i) in (b) of **Hypothesis A** is satisfied then we get

$$\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-} = \mathbf{T}^{\mathbf{u}^+ - \mathbf{v_1}^+}(\mathbf{T}^{\mathbf{v_1}^+} - \mathbf{T}^{\mathbf{v_1}^-}) + \mathbf{T}^{\mathbf{u}^- - \mathbf{v_2}^-}(\mathbf{T}^{\mathbf{v_2}^+} - \mathbf{T}^{\mathbf{v_2}^-}).$$

If, instead (ii) in (b) holds then

$$\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-} = \mathbf{T}^{\mathbf{u}^- - \mathbf{v_1}^-}(\mathbf{T}^{\mathbf{v_1}^+} - \mathbf{T}^{\mathbf{v_1}^-}) + \mathbf{T}^{\mathbf{u}^+ - \mathbf{v_2}^+}(\mathbf{T}^{\mathbf{v_2}^+} - \mathbf{T}^{\mathbf{v_2}^-}).$$

In either case, this shows that the binomial $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-} \in < \mathcal{F} >$ and the proof is complete. □

We now illustrate how we can use all the above results:

Example 13. Let us consider the polynomials

$$f_1 := x_2^{q^2}, \quad f_2 := x_3^{q^3} + x_2^{q^3 - q^2} x_3^{q^2}, \quad f_3 := x_3^q x_2 + x_3 x_2^q \quad \text{and} \quad f_4 := x_3^{q^3} x_2 + x_3 x_2^{q^3}$$

in $\mathbb{F}_{q^2}[x_2, x_3]$. If we consider the graded reverse lexicographic order on $\mathbb{F}_{q^2}[x_2, x_3]$ with $x_2 < x_3$ then the matrix B corresponding to the homomorphism ϕ defined by (1) is

$$\begin{pmatrix} q^2 & 0 & 1 & 1 \\ 0 & q^3 & q & q^3 \end{pmatrix}.$$

The solution set for $B\mathbf{u} = 0$ is a vector space W with dimension 2 and it is not too hard to check that

$$\mathbf{w}_1 = (-1, -1, q^2, 0) = (0, 0, q^2, 0) - (1, 1, 0, 0)$$
$$\mathbf{w}_2 = (-1, -q^2, 0, q^2) = (0, 0, 0, q^2) - (1, q^2, 0, 0)$$

form a basis for W.

Now, we check that the hypothesis of Lemma 12 holds. Note that a linear combination $\alpha_1 \mathbf{w_1} + \alpha_2 \mathbf{w_2}$ belongs to $\mathbb{Z}^4$ if and only if the numbers $-\alpha_1 - \alpha_2$, $-\alpha_1 - \alpha_2 q^2$, $\alpha_1 q^2$ and $\alpha_2 q^2$ are integers. Thus α_1 and α_2 must be integers. Now, let $\mathbf{u} = \alpha_1 \mathbf{w_1} + \alpha_2 \mathbf{w_2} = (-\alpha_1 - \alpha_2, -\alpha_1 - \alpha_2 q^2, \alpha_1 q^2, \alpha_2 q^2) \in \mathbb{Z}^4$. We have to consider four different cases:

(I) For $\alpha_1 \geq 0$ and $\alpha_2 \geq 0$ we get

$$\mathbf{u}^+ = (0, 0, \alpha_1 q^2, \alpha_2 q^2), \qquad \mathbf{u}^- = (\alpha_1 + \alpha_2, \alpha_1 + \alpha_2 q^2, 0, 0)$$
$$(\alpha_1 \mathbf{w_1})^+ = (0, 0, \alpha_1 q^2, 0), \text{ and } (\alpha_2 \mathbf{w_2})^- = (\alpha_2, \alpha_2 q^2, 0, 0).$$

Therefore condition (i) in (b) in Lemma 12 is satisfied.

(II) For $\alpha_1 \leq 0$ and $\alpha_2 \leq 0$ we get

$$\mathbf{u}^+ = (-\alpha_1 - \alpha_2, -\alpha_1 - \alpha_2 q^2, 0, 0), \qquad \mathbf{u}^- = (0, 0, -\alpha_1 q^2, -\alpha_2 q^2)$$
$$(\alpha_1 \mathbf{w_1})^+ = (-\alpha_1, -\alpha_1, 0, 0), \text{ and } (\alpha_2 \mathbf{w_2})^- = (0, 0, 0, -\alpha_2 q^2).$$

Again, we can easily see that the statement (i) in (b) Lemma 12 is satisfied.

(III) If $\alpha_1 < 0$ and $\alpha_2 > 0$, then

$$(\alpha_1 \mathbf{w_1})^- = (0, 0, -\alpha_1 q^2, 0) \quad \text{and} \quad (\alpha_2 \mathbf{w_2})^+ = (0, 0, 0, \alpha_2 q^2).$$

In this case, while determining $\mathbf{u}^+ - (\alpha_2\mathbf{w_2})^+$ and $\mathbf{u}^- - (\alpha_1\mathbf{w_1})^-$, only u_4^+ and u_3^- of $\mathbf{u}^+$ and $\mathbf{u}^-$ are changed. Since $u_4^+ = \alpha_2 q^2$ and $u_3^- = -\alpha_1 q^2$, it follows that condition (ii) in (b) Lemma 12 holds.

(IV) Finally, if $\alpha_1 > 0$ and $\alpha_2 < 0$, then

$$(\alpha_1\mathbf{w_1})^+ = (0, 0, \alpha_1 q^2, 0) \quad \text{and} \quad (\alpha_2\mathbf{w_2})^- = (0, 0, 0, -\alpha_2 q^2).$$

Now, since $u_3^+ = \alpha_1 q^2$ and $u_4^- = -\alpha_2 q^2$, it follows that condition (i) in (b) Lemma 12 holds.

According to Lemma 12, $g_1(t_1, t_2, t_3, t_4) = t_3^q - t_1 t_2$ and $g_2(t_1, t_2, t_3, t_4) = t_4^q - t_1 t_2^q$ generate the kernel of ϕ as an ideal.

We finish this section with a lemma which plays an important role in our proofs. It can be seen as a summary of the discussion made in (Campbell and Wehlau, 2011, page 183).

Lemma 14. *Let $\{x_1, f_2, \ldots, f_m\}$ be a homogeneous SAGBI basis for a graded subalgebra $A \subset \mathbb{F}[x_1, \ldots, x_n]$ using the graded reverse lexicographic order with $x_n > \ldots > x_1$. If, for all $i > 1$, x_1 does not divide $LM(f_i)$, then the ideal $(x_1)_A$ of A generated by x_1 is prime.*

Proof. Let $f, g \in A$ such that $fg \in (x_1)_A$. Since x_1 generates a prime ideal in $\mathbb{F}[x_1, \ldots, x_n]$, we can assume without loss of generality that $g = x_1 g_1$ with $g_1 \in \mathbb{F}[x_1, \ldots, x_n]$. This means that x_1 divides all monomials of g. Hence, at every stage in the subduction of g over $\{x_1, f_2, \ldots, f_m\}$, x_1 will be a factor. Since x_1 does not divide $LM(f_i)$ for all $i > 1$ and $\{x_1, f_2, \ldots, f_m\}$ is a $SAGBI$ basis for A, we can write g as $x_1 g'$ with $g' \in A$. Thus $g \in (x_1)_A$ and this completes the proof. □

3. Invariant Rings

Throughout this section we will always consider the graded reverse lexicographic order on $\mathbb{F}[x_1, \ldots, x_n]$ with $x_1 < x_2 < \cdots < x_n$, where n will be 3 or 4. Therefore if $m_1 = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $m_2 = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ are two distinct monomials, $m_1 <_{grevlex} m_2$ if and only if $a_1 + \cdots + a_n < b_1 + \cdots + b_n$ or $a_1 + \cdots + a_n = b_1 + \cdots + b_n$ and $a_i > b_i$ for the smallest i with $a_i \neq b_i$. We proceed in the following way:
1. we take a finite list of invariant polynomials and then we establish some relations between them. This list will always contain the generators for the invariant field. Now, using the relations we construct an invariant polynomial Θ, whose leading monomial has the form $x_n^{d_n}$.
2. we consider the algebra A generated by some of the polynomials in the list and Θ and show that A is the invariant ring by proving that:

(i) A contains a homogeneous system of parameters;

(ii) the fraction field of A is the invariant field;

(iii) A is integrally closed in its field of fractions.

When constructing the relations between the generators of the invariant rings, we use the endomorphism ψ_1 of $\mathbb{F}[x_1, \ldots, x_n]$ defined by $\psi_1(x_i) = x_i^r - x_1^{r-1} x_i$, where r is the number of elements of the field $\mathbb{F}$. Note that $\psi_1(x_1) = 0$ and $\psi_1(x_2) = x_2^r - x_1^{r-1} x_2$ is the orbit product of x_2 under the action of the group, of lower triangular matrices with ones along the diagonal, $U(n, \mathbb{F})$.

When working with finite unitary groups over the field $\mathbb{F}_{q^2}$ we need the Frobenius map, which will be the equivalent to the complex conjugation when we consider unitary groups over the complex numbers. By considering $\mathbb{F}_{q^2}$ as an algebraic extension of $\mathbb{F}_q$ in degree 2, we define

the Fobenius map $\phi : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ by $\phi(a) := a^q$. This map is an automorphism of order 2 which leaves the elements of $\mathbb{F}_q$ fixed. We shall write $\bar{a}$ instead of a^q.

Let h be the form defining the finite classical group and J the $n \times n$-matrix such that

$$h(v) = v^T J \overline{v} \qquad \text{for all } v \in V,$$

with $\overline{v} = [v_1^q \, v_2^q \cdots v_n^q]^T$. All the Sylow p-groups in this section can easily be obtained by solving the matrix equation

$$N^T J \overline{N} = J,$$

with $N \in U(n, \mathbb{F})$. An explicit matrix description of the Sylow p-subgroups in the general case is given in (Ferreira and Fleischmann, 2016).

3.1. The Invariant Ring of a Sylow p-subgroup of $GU(3, q^2)$

We represent by $h_1 := x_2^{q+1} + x_3^q x_1 + x_3 x_1^q$ the form defining the unitary group $GU(3, q^2)$, hence an invariant polynomial. Also, we denote by G the Sylow p-subgroup of $GU(3, q^2)$. Its elements can be written as

$$\begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ s & -\bar{b} & 1 \end{pmatrix}$$

where $s, b \in \mathbb{F}_{q^2}$ are such that $b\bar{b} + s + \bar{s} = 0$. Therefore, G acts on the polynomial ring $\mathbb{F}_{q^2}[x_1, x_2, x_3]$ in the following way:

$$x_1 \mapsto x_1, \qquad x_2 \mapsto x_2 + bx_1, \qquad x_3 \mapsto x_3 - \bar{b}x_2 + sx_1.$$

Clearly x_1 and the orbit product of x_2 $N(x_2) = \prod_{b \in \mathbb{F}_{q^2}} (x_2 + bx_1) = x_2^{q^2} - x_1^{q^2-1} x_2$ are invariant polynomials. Since

$$h_2 := x_2^{q^3+1} + x_3^{q^3} x_1 + x_3 x_1^{q^3} = \mathcal{P}^q(h_1),$$

h_2 is also invariant under the action of G.

Lemma 15. *The polynomials x_1, $N(x_2)$, h_1 and h_2 satisfy*

$$N(x_2)^{q+1} = h_1^{q^2} - x_1^{q^2-1} h_2 - x_1^{q(q^2-1)} h_1^q + x_1^{(q+1)(q^2-1)} h_1.$$

Proof. A straightforward calculation shows that

$$\psi_1(h_1) = h_1^{q^2} - x_1^{q^2-1} h_2 - x_1^{q(q^2-1)} h_1^q + x_1^{(q+1)(q^2-1)} h_1.$$

Since $\psi_1(x_1) = 0$ and $\psi_1(x_2) = x_2^{q^2} - x_1^{q^2-1} x_2 = N(x_2)$ we obtain

$$N(x_2)^{q+1} = h_1^{q^2} - x_1^{q^2-1} h_2 - x_1^{q(q^2-1)} h_1^q + x_1^{(q+1)(q^2-1)} h_1$$

and the proof is completed. □

Lemma 16. *The polynomial h_2 can be written as $h_2 = h_1^{q^2-q+1} + x_1\Theta$ where Θ is the invariant polynomial*

$$\Theta := x_3^{q^3} + x_1^{q^3-1} x_3 - x_2^{q^3-q} X - (x_1 X + x_2^{q+1}) \sum_{i=1}^{q-1} (-1)^i x_2^{(q^2+q)(q-1-i)} x_1^{qi-1} X^{qi}.$$

Proof. For simplicity write $X = x_3^q + x_1^{q-1} x_3$. Hence $h_1 = x_2^{q+1} + x_1 X$ and

$$
\begin{aligned}
h_1^{q^2-q+1} &= (x_2^{q+1}+x_1X)^{q^2-q+1} = (x_2^{q+1}+x_1X)(x_2^{q^2+q}+x_1^qX^q)^{q-1}\\
&= (x_2^{q+1}+x_1X)\sum_{i=0}^{q-1}(-1)^i x_2^{(q^2+q)(q-1-i)}x_1^{qi}X^{qi}\\
&= (x_2^{q+1}+x_1X)\left(x_2^{q^3-q}+x_1\sum_{i=1}^{q-1}(-1)^i x_2^{(q^2+q)(q-1-i)}x_1^{qi-1}X^{qi}\right)\\
&= x_2^{q^3+1}+x_1\left(x_2^{q^3-q}X+(x_1X+x_2^{q+1})\sum_{i=1}^{q-1}(-1)^i x_2^{(q^2+q)(q-1-i)}x_1^{q(i-1)}X^{qi}\right).
\end{aligned}
$$

Hence $h_2 - h_1^{q^2-q+1} = x_1\Theta$ where

$$\Theta := x_3^{q^3} + x_1^{q^3-1}x_3 - x_2^{q^3-q}X - (x_1X+x_2^{q+1})\sum_{i=1}^{q-1}(-1)^i x_2^{(q^2+q)(q-1-i)}x_1^{qi-1}X^{qi}.$$

Since x_1, h_1 and h_2 are invariant, the polynomial Θ is also invariant. □

Let A denote the $\mathbb{F}_{q^2}$-algebra generated by x_1, $N(x_2)$, h_1 and Θ, i.e.,

$$A = \mathbb{F}_{q^2}[x_1, N(x_2), h_1, \Theta].$$

Obviously, $A \subseteq \mathbb{F}_{q^2}[x_1,x_2,x_3]^G$. Our goal is to prove that A is equal to $\mathbb{F}_{q^2}[x_1,x_2,x_3]^G$.

Lemma 17. *The following relation*

$$h_1^{q^2} - N(x_2)^{q+1} - x_1^{q^2-1}h_1^{q^2-q+1} - x_1^{q^2}\Theta - x_1^{q(q^2-1)}h_1^q + x_1^{(q+1)(q^2-1)}h_1 = 0 \tag{2}$$

is a subduction of $h_1^{q^2} - N(x_2)^{q+1}$ over $\{x_1, N(x_2), h_1, \Theta\}$.
Furthermore, $\{x_1, N(x_2), h_1, \Theta\}$ is a SAGBI basis for A.

Proof. According to Lemma 16, $h_2 = h_1^{q^2-q+1} + x_1\Theta$. Thus if in Lemma 15 we substitute h_2 by $h_1^{q^2-q+1} + x_1\Theta$, then we get the relation in the lemma. The relation (2) is in fact a subduction of $h_1^{q^2} - N(x_2)^{q+1}$ over $\{x_1, N(x_2), h_1, \Theta\}$.

We keep the notation of Section 2. It is not hard to check that

$$LM(N(x_2)) = x_2^{q^2}, \quad LM(h_1) = x_2^{q+1}, \quad \text{and } LM(\Theta) = x_3^{q^3}$$

and therefore the matrix B corresponding to the homomorphism ϕ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & q^2 & q+1 & 0 \\ 0 & 0 & 0 & q^3 \end{pmatrix}.$$

The solution set for $B\mathbf{u} = 0$ is a vector space W with dimension 1 and it is easy to check that

$$\mathbf{w} = (0, -q-1, q^2, 0) = (0,0,q^2,0) - (0,q+1,0,0)$$

is a basis for W. Now, $\alpha\mathbf{w} \in \mathbb{Z}^4$ if and only if $-\alpha q - \alpha$ and αq^2 are integers. This can only happen when $\alpha \in \mathbb{Z}$. Hence according to Lemma 11

$$\mathbf{T}^{\mathbf{w}^+} - \mathbf{T}^{\mathbf{w}^-} = t_3^{q^2} - t_2^{q+1} =: g(t_1,t_2,t_3,t_4)$$

generates the kernel of ϕ. We have seen that $g(x_1, N(x_2), h_1, \Theta) = h_1^{q^2} - N(x_2)^{q+1}$ has a subduction over $\{x_1, N(x_2), h_1, \Theta\}$ that terminates at zero. Thus it follows from Theorem 6 that $\{x_1, N(x_2), h_1, \Theta\}$ is a $SAGBI$ basis for A. □

Theorem 18. *The invariant ring for the Sylow p-subgroup G of $GU(3,q^2)$ is generated by x_1, $N(x_2)$, h_1 and Θ, i.e., $\mathbb{F}_{q^2}[x_1,x_2,x_3]^G = \mathbb{F}_{q^2}[x_1,N(x_2),h_1,\Theta]$, Furthermore, the generators satisfy (2).*

Proof. Applying (Campbell and Wehlau, 2011, Lemma 2.6.3) we see that $\{x_1, N(x_2), h_1, \Theta\}$ contains a homogeneous system of parameters for $\mathbb{F}_{q^2}[x_1,x_2,x_3]^G$, namely $\{x_1, N(x_2), \Theta\}$. Hence, $\mathbb{F}_{q^2}[x_1,x_2,x_3]$ is integral over A. From Theorem 2 we get $\mathbb{F}_{q^2}(x_1,x_2,x_3)^G = \mathbb{F}_{q^2}(x_1,N(x_2),h_1)$. Since $\mathbb{F}_{q^2}(x_1,N(x_2),h_1) \subset \mathrm{Quot}(A) \subset \mathbb{F}_{q^2}(x_1,x_2,x_3)^G$, we conclude that A and $\mathbb{F}_{q^2}[x_1,x_2,x_3]^G$ have the same fraction field. Now, it remains to prove that A is integrally closed. Since x_1 is invertible in $A[x_1^{-1}]$, from (2) we get $\Theta \in \mathbb{F}_{q^2}[x_1,N(x_2),h_1][x_1^{-1}]$. Hence

$$A[x_1^{-1}] = \mathbb{F}_{q^2}[x_1,N(x_2),h_1][x_1^{-1}]$$

which is a localisation of a polynomial ring and therefore it is a Unique Factorisation Domain. From Lemmas 17 and 14 it follows that the ideal of A generated by x_1 is prime. Hence A is integrally closed (see Benson, 1993, Proposition 6.3.1) and this finishes the proof. □

Remark 19. We would like to note that $\{x_1, N(x_2), h_1, N(x_3)\}$ also generates the invariant ring $\mathbb{F}_{q^2}[x_1,x_2,x_3]^G$, where $N(x_3)$ is the orbit product of x_3. Actually it is not hard to see that Θ is divisible by x_3 and therefore by $N(x_3)$. Since they are monic polynomials of the same degree in x_3 we conclude that $\Theta = N(x_3)$.

Finally, we show that the invariant ring for G is a complete intersection. It is actually an hypersurface. Consider the polynomial ring $\mathbb{F}_{q^2}[X_1,X_2,X_3,X_4]$ and the homomorphism $\Phi : \mathbb{F}_{q^2}[X_1,X_2,X_3,X_4] \longrightarrow A$ defined by

$$X_1 \mapsto x_1, \quad X_2 \mapsto N(x_2), \quad X_3 \mapsto h_1, \quad X_4 \mapsto \Theta.$$

Lemma 20. *The kernel of Φ is generated by the polynomial*

$$\begin{aligned} P(X_1,X_2,X_3,X_4) := &- X_1^{q^2}X_4 + X_3^{q^2} - X_2^{q+1} - X_1^{q^2-1}X_3^{q^2-q+1} \\ &- X_1^{q(q^2-1)}X_3^q + X_1^{(q+1)(q^2-1)}X_3. \end{aligned}$$

Moreover, A is a complete intersection ring.

Proof. It follows from (2) that $P(X_1,X_2,X_3,X_4)$ belongs to the kernel of Φ. Note that the polynomial $P(X_1,X_2,X_3,X_4)$ is linear in X_4 and X_1 is the only irreducible dividing the coefficient of X_4. Since X_1 does not divide the X_4-constant term, we conclude that $P(X_1,X_2,X_3,X_4)$ is irreducible in $\mathbb{F}_{q^2}[X_1,X_2,X_3,X_4]$. Therefore it generates a prime ideal. Now, the Krull dimension of A is 3 (see Smith, 1995, Corollary 5.3.5). Since $\mathbb{F}_{q^2}[X_1,X_2,X_3,X_4]/\ker\Phi \simeq A$, the kernel of Φ will be a prime ideal with height 1. Hence it is generated by $P(X_1,X_2,X_3,X_4)$ and therefore A is a complete intersection ring. □

3.2. The Invariant Ring of a Sylow p-subgroup of $GU(4,q^2)$

We represent by $h_1 := x_3^q x_2 + x_3 x_2^q + x_4^q x_1 + x_4 x_1^q$ the form defining the unitary group $GU(4,q^2)$. Let G be the Sylow p-subgroup of $GU(4,q^2)$. Its elements can be written as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ b_1 & 1 & 0 & 0 \\ b_2 & c & 1 & 0 \\ s & -\bar{b}_1 c - \bar{b}_2 & -\bar{b}_1 & 1 \end{pmatrix}$$

where $b_1, b_2, c, s \in \mathbb{F}_{q^2}$ such that $c + \bar{c} = 0$ and $s + \bar{s} = -b_1\bar{b}_2 - b_2\bar{b}_1$. The orbit products of x_2 and x_3 are

$$N(x_2) = x_2^{q^2} - x_1^{q^2-1}x_2,$$
$$N(x_3) = (x_3^{q^2} - x_1^{q^2-1}x_3)^q + N(x_2)^{q-1}(x_3^{q^2} - x_1^{q^2-1}x_3)$$

respectively. Since h_1 is clearly an invariant, it follows that the polynomials

$$h_2 = x_3^{q^3}x_2 + x_3x_2^{q^3} + x_4^{q^3}x_1 + x_4x_1^{q^3} = \mathcal{P}^q(h_1),$$
$$h_3 = x_3^{q^5}x_2 + x_3x_2^{q^5} + x_4^{q^5}x_1 + x_4x_1^{q^5} = \mathcal{P}^{q^3}(h_2),$$

are also invariant under the action of G.

Lemma 21. *We have* $N(x_2)N(x_3) = h_1^{q^2} - x_1^{q^2-1}h_2 - x_1^{q(q^2-1)}h_1^q + x_1^{(q+1)(q^2-1)}h_1$ *and*

$$N(x_2)N(x_3)^{q^2} - N(x_2)^{q^3-q^2+1}N(x_3)^q + N(x_2)^{q^3-q+1}N(x_3)$$
$$= h_2^{q^2} - x_1^{q^2-1}h_3 - x_1^{q^3(q^2-1)}h_1^{q^2} + x_1^{(q^3+1)(q^2-1)}h_2.$$

Proof. First, we note that $\psi_1(x_2) = x_2^{q^2} - x_1^{q^2-1}x_2 = N(x_2)$ and if we consider $X = x_3^{q^2} - x_1^{q^2-1}x_3$, then $\psi_1(x_3) = X$. Therefore

$$N(x_2)N(x_3) = N(x_2)(X^q + N(x_2)^{q-1}X) = N(x_2)X^q + N(x_2)^qX$$
$$= \psi_1(x_3)^q\psi_1(x_2) + \psi_1(x_3)\psi_1(x_2)^q = \psi_1(h_1).$$

It can easily be checked that

$$\psi_1(h_1) = h_1^{q^2} - x_1^{q^2-1}h_2 - x_1^{q(q^2-1)}h_1^q + x_1^{(q+1)(q^2-1)}h_1.$$

Finally, we have

$$N(x_2)N(x_3)^{q^2} - N(x_2)^{q^3-q^2+1}N(x_3)^q + N(x_2)^{q^3-q+1}N(x_3) =$$
$$N(x_2)X^{q^3} + N(x_2)^{q^3}X = \psi_1(h_2).$$

Now, an easy calculation shows that

$$\psi_1(h_2) = h_2^{q^2} - x_1^{q^2-1}h_3 - x_1^{q^3(q^2-1)}h_1^{q^2} + x_1^{(q^3+1)(q^2-1)}h_2.$$

□

If we consider the modulo x_1 reductions of $N(x_2), N(x_3), h_1, h_2$ and h_3, then we obtain polynomials

$$f_1 := x_2^{q^2},\ f_2 := x_3^{q^3} + x_2^{q^3-q^2}x_3^{q^2},\ f_3 := x_3^qx_2 + x_3x_2^q$$
$$f_4 := x_3^{q^3}x_2 + x_3x_2^{q^3} \quad \text{and} \quad f_5 := x_3^{q^5}x_2 + x_3x_2^{q^5}.$$

We consider the graded reverse lexicographic order on $\mathbb{F}_{q^2}[x_2, x_3]$ with $x_2 < x_3$.

Lemma 22. *The set* $\{f_1, f_2, f_3, f_4\}$ *is a SAGBI basis for* $\mathbb{F}_{q^2}[f_1, f_2, f_3, f_4]$ *and the polynomial* f_5 *has a subduction over* $\{f_1, f_2, f_3, f_4\}$ *that terminates at zero.*

Proof. Let A' denote the algebra $\mathbb{F}_{q^2}[f_1, f_2, f_3, f_4]$ and $C = \{f_1, f_2, f_3, f_4\}$.

We proceed as in Lemma 17 to show that C is a $SAGBI$ basis for A'. Here the matrix B is

$$\begin{pmatrix} q^2 & 0 & 1 & 1 \\ 0 & q^3 & q & q^3 \end{pmatrix}$$

and in Example 13 we proved that

$$g_1(t_1,t_2,t_3,t_4) = t_3^{q^2} - t_1t_2 \text{ and } g_2(t_1,t_2,t_3,t_4) = t_4^{q^2} - t_1t_2^{q^2}$$

generate the $\ker\phi$. It follows from Lemma 21 that

$$f_3^{q^2} - f_1f_2 = 0 \tag{3}$$

$$f_4^{q^2} - f_1f_2^{q^2} - f_1^{q^3-q^2+1}f_2^q + f_1^{q^3-q+1}f_2 = 0. \tag{4}$$

It is not hard to see that (3) and (4) are a subduction over C of $g_1(f_1,f_2,f_3,f_4)$ and $g_2(f_1,f_2,f_3,f_4)$, respectively. Hence C is a $SAGBI$ basis for A'.

Finally, we show that $f_5 \in A'$ and from this, we conclude that the polynomial f_5 has a subduction over $\{f_1,f_2,f_3,f_4\}$ terminating at zero. A straightforward calculation shows that

$$\begin{pmatrix} f_3 & f_3^q \\ f_4 & f_3^{q^2} \\ f_5 & f_4^{q^2} \end{pmatrix} = \begin{pmatrix} x_3^q & x_2^q \\ x_3^{q^3} & x_2^{q^3} \\ x_3^{q^5} & x_2^{q^5} \end{pmatrix} \begin{pmatrix} x_2 & x_2^{q^2} \\ x_3 & x_3^{q^2} \end{pmatrix}.$$

Thus if we take

$$f := f_3^{q^2+1} - f_4f_3^q = \begin{vmatrix} x_3^q & x_2^q \\ x_3^{q^3} & x_2^{q^3} \end{vmatrix} \begin{vmatrix} x_2 & x_2^{q^2} \\ x_3 & x_3^{q^2} \end{vmatrix} = -\begin{vmatrix} x_2 & x_2^{q^2} \\ x_3 & x_3^{q^2} \end{vmatrix}^{q+1}$$

and

$$g := f_4^{q^2+1} - f_3^{q^2}f_5 = \begin{vmatrix} x_3^{q^3} & x_2^{q^3} \\ x_3^{q^5} & x_2^{q^5} \end{vmatrix} \begin{vmatrix} x_2 & x_2^{q^2} \\ x_3 & x_3^{q^2} \end{vmatrix} = -\begin{vmatrix} x_2 & x_2^{q^2} \\ x_3 & x_3^{q^2} \end{vmatrix}^{q^3+1}$$

we obtain $0 = f^{q^2-q+1} - g$. Therefore $f_3^{q^2}f_5 = f_4^{q^2+1} - f_3^{q^3-q^2+q}(f_3^{q^2-q+1} - f_4)^{q^2-q+1}$. From (3) and (4) we conclude that $f_4^{q^2}$ is divisible by $f_3^{q^2}$. Hence $f_5 \in A'$ and this finishes the proof. □

It follows from the previous Lemma that there exists a subduction of f_5 over $\{f_1,f_2,f_3,f_4\}$, i.e., a polynomial $P(X_1,X_2,X_3,X_4)$ such that $f_5 = P(f_1,f_2,f_3,f_4)$.

Note that $h_1 = f_3 + x_1(x_4^q + x_1^{q-1}x_4)$ and $h_2 = f_4 + x_1(x_4^{q^3} + x_1^{q^3-1}x_4)$. Since the variable x_4 does not appear in $N(x_2)$ and $N(x_3)$ we can conclude that the monomial $x_1x_4^{q^5}$ will not occur in $P(N(x_2),N(x_3),h_1,h_2)$. Hence we get

$$h_3 = f_5 + x_1(x_4^{q^5} + x_1^{q^5-1}x_4) = P(N(x_2),N(x_3),h_1,h_2) + x_1\Theta,$$

with $\Theta := x_4^{q^5} + x_1^{q^5-1}x_4 + \cdots$ an invariant polynomial under the action of G. Let A be the $\mathbb{F}_{q^2}$-algebra generated by the polynomials x_1, $N(x_2)$, $N(x_3)$, h_1, h_2 and Θ. We shall prove that A is the invariant ring for the Sylow p-subgroup of $GU(4,q^2)$.

Lemma 23. *The following relations*

$$h_1^{q^2} - N(x_2)N(x_3) - x_1^{q^2-1}h_2 - x_1^{q(q^2-1)}h_1^q + x_1^{(q+1)(q^2-1)}h_1 = 0 \tag{5}$$

and

$$\begin{aligned} h_2^{q^2} - N(x_2)N(x_3)^{q^2} + N(x_2)^{q^3-q^2+1}N(x_3)^q - N(x_2)^{q^3-q+1}N(x_3) \\ - x_1^{q^2-1}P(N(x_2),N(x_3),h_1,h_2) - x_1^{q^2}\Theta - x_1^{q^3(q^2-1)}h_1^{q^2} + x_1^{(q^3+1)(q^2-1)}h_2 = 0 \end{aligned} \tag{6}$$

are a subduction over $\{x_1,N(x_2),N(x_3),h_1,h_2,\Theta\}$ *of* $h_1^{q^2} - N(x_2)N(x_3)$ *and* $h_2^{q^2} - N(x_2)N(x_3)^{q^2}$*,respectively. Furthermore,* $\{x_1,N(x_2),N(x_3),h_1,h_2,\Theta\}$ *is a SAGBI basis for* A.

Proof. Since $P(f_1, f_2, f_3, f_4)$ is a subduction of f_5 over $\{f_1, f_2, f_3, f_4\}$ and $h_3 = f_5 + x_1(x_4^{q^5} + x_1^{q^5-1}x_4) = P(N(x_2), N(x_3), h_1, h_2) + x_1\Theta$ we see that

$$x_1^{q^2-1}P(N(x_2), N(x_3), h_1, h_2) + x_1^{q^2}\Theta$$

is a subduction of $x_1^{q^2-1}h_3$ over $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$. Hence (5) and (6) are a subduction over $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$ of $h_1^{q^2} - N(x_2)N(x_3)$ and $h_2^{q^2} - N(x_2)N(x_3)^{q^2}$, respectively. The matrix B corresponding to the homomorphism ϕ in (1) is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & q^2 & 0 & 1 & 1 & 0 \\ 0 & 0 & q^3 & q & q^3 & 0 \\ 0 & 0 & 0 & 0 & 0 & q^5 \end{pmatrix}.$$

Analogously to what was done in the proof Lemma 22, we can show that the vectors

$$\mathbf{w}_1 = (0, -1, -1, q^2, 0, 0) = (0, 0, 0, q^2, 0, 0) - (0, 1, 1, 0, 0, 0)$$
$$\mathbf{w}_2 = (0, -1, -q^2, 0, q^2, 0) = (0, 0, 0, 0, q^2, 0) - (0, 1, q^2, 0, 0, 0)$$

form a basis for the solution set of $B\mathbf{u} = 0$ and that

$$g_1(t_1, t_2, t_3, t_4, t_5, t_6) = t_4^{q^2} - t_2t_3,$$
$$g_2(t_1, t_2, t_3, t_4, t_5, t_6) = t_5^{q^2} - t_2t_3^{q^2}$$

generate $\ker\phi$. In the beginning of the proof we proved that

$$h_1^{q^2} - N(x_2)N(x_3) = g_1(x_1, N(x_2), N(x_3), h_1, h_2, \Theta),$$
$$h_2^{q^2} - N(x_2)N(x_3)^{q^2} = g_2(x_1, N(x_2), N(x_3), h_1, h_2, \Theta)$$

have a subduction over $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$ that terminates at zero. This finishes the proof. □

Theorem 24. *The invariant ring for the Sylow p-subgroup G of $GU(4, q^2)$ is generated by x_1, $N(x_2)$, $N(x_3)$, h_1, h_2 and Θ, i.e.,*

$$R := \mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]^G = \mathbb{F}_{q^2}[x_1, N(x_2), N(x_3), h_1, h_2, \Theta],$$

Furthermore, the generators satisfy the relations (5) and (6).

Proof. Since $\{x_1, N(x_2), N(x_3), \Theta\}$ is a homogeneous system of parameters for R (see Campbell and Wehlau, 2011, Lemma 2.6.3), the polynomial ring $\mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]$ is integral over A. According to Theorem 2 we have $\mathbb{F}_{q^2}(x_1, x_2, x_3, x_4)^G = \mathbb{F}_{q^2}(x_1, N(x_2), N(x_3), h_1)$. Since

$$\mathbb{F}_{q^2}(x_1, N(x_2), N(x_3), h_1) \subset \mathrm{Quot}(A) \subset \mathbb{F}_{q^2}(x_1, x_2, x_3, x_4)^G,$$

we conclude that $\mathrm{Quot}(A)$ is equal to $\mathbb{F}_{q^2}(x_1, x_2, x_3, x_4)^G$. It follows from (5) and (6) that $h_2, \Theta \in \mathbb{F}_{q^2}[x_1, N(x_2), h_1][x_1^{-1}]$. Hence $A[x_1^{-1}] = \mathbb{F}_{q^2}[x_1, N(x_2), N(x_3), h_1][x_1^{-1}]$ which is the localisation of a polynomial ring and therefore a Unique Factorisation Domain. Applying Lemmas 23 and 14 we conclude that the ideal of A generated by x_1 is prime. Hence A is integrally closed (see Benson, 1993, Proposition 6.3.1). □

Remark 25. Note that $C = \{x_1, N(x_2), N(x_3), h_1, h_2, N(x_4)\}$ is also a generating set for the invariant ring $\mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]^G$, where $N(x_4)$ is the orbit product of x_4. In fact, it is not hard to see that $N(x_4) \in A$ has the same leading monomial as Θ and therefore C is a $SAGBI$ basis for $A = \mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]^G$. Hence C is also a generating set for A.

We finish this section by showing that the invariant ring for G is a complete intersection. Consider the ring $\mathbb{F}_{q^2}[X_1, X_2, X_3, X_4, Z_1, Z_2]$ and the homomorphism

$$\Phi : \mathbb{F}_{q^2}[X_1, X_2, X_3, X_4, Z_1, Z_2] \longrightarrow A$$

defined by

$$X_1 \mapsto x_1,\ X_2 \mapsto N(x_2),\ X_3 \mapsto N(x_3),\ X_4 \mapsto \Theta,\ Z_1 \mapsto h_1,\ Z_2 \mapsto h_2.$$

Lemma 26. *The kernel of Φ is generated by the polynomials*

$$P_1(X_1, X_2, X_3, X_4, Z_1, Z_2) :=$$
$$Z_1^{q^2} - X_2X_3 - X_1^{q^2-1}Z_2 - X_1^{q(q^2-1)}Z_1^q + X_1^{(q+1)(q^2-1)}Z_1$$

and

$$P_2(X_1, X_2, X_3, X_4, Z_1, Z_2) := Z_2^{q^2} - X_2X_3^{q^2} + X_2^{q^3-q^2+1}X_3^q - X_2^{q^3-q+1}X_3$$
$$- X_1^{q^2-1}P(X_2, X_3, Z_1, Z_2) - X_1^{q^2}X_4 - X_1^{q^3(q^2-1)}Z_1^{q^2} + X_1^{(q^3+1)(q^2-1)}Z_2$$

where the polynomial P is such that $h_3 = P(N(x_2), N(x_3), h_1, h_2) + x_1\Theta$. Moreover, A is a complete intersection.

Proof. Let $R := \mathbb{F}_{q^2}[X_1, X_2, X_3, X_4, Z_1, Z_2]$. The Krull dimension of A is 4 (see Smith, 1995, Corollary 5.3.5). Since $R/\ker\Phi \simeq A$, the kernel of Φ is a prime ideal of height 2. From (5) and (6) we see that P_1 and P_2 are elements in the kernel of Φ. We shall prove that P_1, P_2 is a regular sequence in R and that the ideal $I = (P_1, P_2)$ is prime. Then it will follow that I has height 2 and therefore $\ker\Phi = I$. Obviously $R/(X_1)$ is an integral domain. The modulo X_1 reductions of P_1 and P_2 are

$$\overline{P}_1 = \overline{Z}_1^{q^2} - \overline{X}_2\overline{X}_3 \text{ and } \overline{P}_2 = \overline{Z}_2^{q^2} - \overline{X}_2\overline{X}_3^{q^2} + \overline{X}_2^{q^3-q^2+1}\overline{X}_3^q - \overline{X}_2^{q^3-q+1}\overline{X}_3,$$

respectively. It is clear that $\overline{X}_2, \overline{X}_3, \overline{X}_4, \overline{P}_1, \overline{P}_2$ is an homogeneous system of parameters of the polynomial, hence Cohen-Macaulay, ring $R/(X_1)$ and therefore a regular sequence. Thus, $\overline{P}_1, \overline{P}_2$ is also regular in $R/(X_1)$. Hence X_1, P_1, P_2 is a regular sequence in R and since they are homogeneous polynomials, P_1, P_2, X_1 is also a regular sequence. Then it follows that, in particular, P_1, P_2 is a regular sequence and that $R/(P_1, P_2)$ is embedded into $R/(P_1, P_2)[\bar{X}_1^{-1}]$. Now, using P_1 and P_2 we can eliminate $\bar{Z}_2$ and $\bar{X}_4$, respectively. Hence

$$R/(P_1, P_2)[\bar{X}_1^{-1}] = \mathbb{F}_{q^2}[\bar{X}_1, \bar{X}_2, \bar{X}_3, \bar{Z}_1][\bar{X}_1^{-1}]$$

which is of Krull dimension greater than or equal to 4 and therefore equal to 4. Therefore $R/(P_1, P_2)[\bar{X}_1^{-1}]$ is the localisation of a polynomial ring, thus a domain. Hence (P_1, P_2) is a prime ideal and therefore A is a complete intersection. □

3.3. The Invariant Ring of a Sylow p-subgroup of $Sp(4, q)$

We represent by $h_1 := x_3^q x_2 - x_3 x_2^q + x_4^q x_1 - x_4 x_1^q$ the form invariant under the action of the symplectic group $Sp(4, q)$. Let G be the Sylow p-subgroup of $Sp(4, q)$, whose elements can be written as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ b_1 & 1 & 0 & 0 \\ b_2 & c & 1 & 0 \\ s & -b_1c + b_2 & -b_1 & 1 \end{pmatrix}$$

with $b_1, b_2, c, s \in \mathbb{F}_q$. The orbit products of x_2 and x_3 are

$$N(x_2) = x_2^q - x_1^{q-1}x_2,$$
$$N(x_3) = (x_3^q - x_1^{q-1}x_3)^q - N(x_2)^{q-1}(x_3^q - x_1^{q-1}x_3),$$

respectively. Since h_1 is invariant, the polynomials

$$h_2 = x_3^{q^2}x_2 - x_3x_2^{q^2} + x_4^{q^2}x_1 - x_4x_1^{q^2} = \mathcal{P}^q(h_1),$$
$$h_3 = x_3^{q^3}x_2 - x_3x_2^{q^3} + x_4^{q^3}x_1 - x_4x_1^{q^3} = \mathcal{P}^{q^2}(h_2)$$

are also invariant.

One can show that $h_3 = P(N(x_2), N(x_3), h_1, h_2) + x_1\Theta$, where $\Theta := x_4^{q^3} - x_1^{q^3-1}x_4 + \cdots$ is an invariant polynomial under the action of G.

Theorem 27. *The invariant ring for the Sylow p-subgroup G of $Sp(4, q)$ is generated by x_1, $N(x_2)$, $N(x_3)$, h_1, h_2 and Θ, i.e.,*

$$\mathbb{F}_q[x_1, x_2, x_3, x_4]^G = \mathbb{F}_q[x_1, N(x_2), N(x_3), h_1, h_2, \Theta].$$

These generators satisfy

$$h_1^q - N(x_2)N(x_3) - x_1^{q-1}h_2 + x_1^{q(q-1)}h_1 = 0$$

and

$$h_2^q - N(x_2)N(x_3)^q - N(x_2)^{q^2-q+1}N(x_3) - x_1^{q-1}P(N(x_2), N(x_3), h_1, h_2) - x_1^q\Theta - x_1^{q(q-1)}h_1^q + x_1^{(q^2+1)(q-1)}h_2 = 0.$$

Furthermore, $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$ is a SAGBI basis and the invariant ring is a complete intersection.

The full details of this subsection can be found at Subsection 4.3 in (Ferreira, 2011).

3.4. The Invariant Ring of a Sylow p-subgroup of $O^+(4, q)$ with q odd

Let $h_1 := x_3x_2 + x_4x_1$ be the form defining the orthogonal group $O^+(4, q)$ with q odd, and G be a Sylow p-subgroup of $O^+(4, q)$ with q odd, whose elements can be written as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ b_1 & 1 & 0 & 0 \\ b_2 & 0 & 1 & 0 \\ -b_1b_2 & -b_2 & -b_1 & 1 \end{pmatrix}$$

with $b_1, b_2 \in \mathbb{F}_q$. It is not hard to see that the orbit products of x_2 and x_3 are $N(x_2) = x_2^q - x_1^{q-1}x_2$ and $N(x_3) = x_3^q - x_1^{q-1}x_3$, respectively. The polynomials

$$h_2 = x_3^qx_2 + x_3x_2^q + x_4^qx_1 + x_4x_1^q = \mathcal{P}^q(h_1),\ h_3 = x_3^{q^2}x_2 + x_3x_2^{q^2} + x_4^{q^2}x_1 + x_4x_1^{q^2} = \mathcal{P}^{q^2}(h_2)$$

are invariant.

Theorem 28. *The invariant ring for the Sylow p-subgroup G of $O^+(4, q)$ is generated by x_1, $N(x_2)$, $N(x_3)$, h_1, h_2 and Θ, i.e.,*

$$\mathbb{F}_q[x_1, x_2, x_3, x_4]^G = \mathbb{F}_q[x_1, N(x_2), N(x_3), h_1, h_2, \Theta],$$

These generators satisfy $h_1^q - N(x_2)N(x_3) - x_1^{q-1}h_2 + x_1^{2q-2}h_1 = 0$ *and*

$$h_2^q - N(x_2)N(x_3)^q - N(x_2)^q N(x_3) - x_1^{q-1}P(N(x_2), N(x_3), h_1, h_2) - x_1^q\Theta - 2x_1^{q(q-1)}h_1^q + x_1^{(q+1)(q-1)}h_2 = 0.$$

Furthermore, $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$ *is a SAGBI basis and the invariant ring is a complete intersection.*

The full details of this subsection can be found in Subsection 4.4 of (Ferreira, 2011).

References

Benson, D., 1993. Polynomial Invariants of Finite Groups. Vol. 190 of London Mathematical Society Lecture Notes Series. Cambridge University Press, Cambridge.

Bosma, W., Cannon, J. J., Playoust, C., 1997. The Magma algebra system I: the user language. J. Symb. Comput., 24, 235-265.

Carlisle, D., Kropholler, P. H., 1992. Modular invariants of finite symplectic groups. Preprint.

Campbell, H.E.A., Wehlau, D., 2011. Modular Invariant Theory. Vol. 139 of Encyclopaedia of Mathematical Sciences. Springer-Verlag.

Ferreira, J. N. M., 2011. On invariant rings of sylow subgroups of finite classical groups. PhD Thesis, University of Kent. http://hdl.handle.net/10400.13/177.

Ferreira, J. N. M., Fleischmann, P., 2016. The invariant fields of the sylow groups of classical groups in the natural characteristic. Communications in Algebra 44:3, 977-1010. http://dx.doi.org/10.1080/00927872.2014.999922

Huah, C., Shin-Yao, J., 2006. Polynomial invariants of finite unitary groups. Journal of Algebra 302, 686-719.

Kapur, D.,Madlener, K., 1989. A completion procedure for computing a canonical basis for a k-subalgebra. In: E. Kaltofen, S. W. (Ed.), Proceedings of Computers and Mathematics. MIT, Cambridge, Mass., pp. 1-11.

Robbiano, L., Sweedler, M., 1990. Subalgebras bases. In: Lecture Notes in Mathematics. Vol. 1430. Springer-Verlag, Berlin, pp. 6187.

Smith, L., 1995. Polynomial Invariants of Finite Groups. A. K. Peters, Wellesley, Mass.

Sturmfels, B., 1996. Gröbner Bases and Convex Polytopes. Vol. 8 of University Lecture Series. American Mathematical Society.