

On Invariant Rings of Sylow Subgroups of Finite Classical Groups

by
Jorge Nélio Marques Ferreira

A thesis submitted for the Degree of Doctor in Philosophy in the
subject of Pure Mathematics.

School of Mathematics, Statistics and Actuarial Science,
University of Kent,
Canterbury.

March 2011

Declaration

I declare that, to the best of my knowledge, the material contained in this thesis is original work of the author. I have clearly stated any contributions, in jointly-authored works, as well as referenced the contributions of other people working in the area. Also, I have not presented this work elsewhere for a degree, diploma, or similar qualification in another university or similar institution.

Abstract

In this thesis we study the invariant rings for the Sylow p -subgroups of the finite classical groups. We have successfully constructed presentations for the invariant rings for the Sylow p -subgroups of the unitary groups $GU(3, \mathbb{F}_{q^2})$ and $GU(4, \mathbb{F}_{q^2})$, the symplectic group $Sp(4, \mathbb{F}_q)$ and the orthogonal group $O^+(4, \mathbb{F}_q)$ with q odd. In all cases, we obtained a minimal generating set which is also a *SAGBI* basis. Moreover, we computed the relations among the generators and showed that the invariant ring for these groups are a complete intersection. This shows that, even though the invariant rings of the Sylow p -subgroups of the general linear group are polynomial, the same is not true for Sylow p -subgroups of general classical groups.

We also constructed the generators for the invariant fields for the Sylow p -subgroups of $GU(n, \mathbb{F}_{q^2})$, $Sp(2n, \mathbb{F}_q)$, $O^+(2n, \mathbb{F}_q)$, $O^-(2n+2, \mathbb{F}_q)$ and $O(2n+1, \mathbb{F}_q)$, for every n and q . This is an important step in order to obtain the generators and relations for the invariant rings of all these groups.

Acknowledgements

I am very grateful to my supervisor Professor Peter Fleischmann for his incredible support, his valuable advice and his never ending patience. I would also like to express my gratitude to my second supervisor Dr. James Shank for various and helpful comments.

I would like to thank Universidade da Madeira, in particular its Centro de Ciências Exactas e da Engenharia and the former Departamento de Matemática e Engenharias for always supporting my academic career. I thank all my colleagues and friends for their support. In particular, a special thank to Professor José Carmo for his help throughout the years. Also, I thank Professor José Castanheira da Costa for getting me interested in invariant theory.

I also would like to thank the School of Mathematics, Statistics and Actuarial Science at the University of Kent for providing me with the necessary conditions to carry out my research.

I wish to thank Fundação para a Ciência e Tecnologia for the financial support provided, through Programa Operacional Potencial Humano (POPH) do Fundo Social Europeu (FSE), by the grant SFRH/BD/30132/2006.

To my friends, who are too numerous to be listed here, I thank you all for helping me in some many and different ways. You will never be forgotten.

Finally, but not least, to my parents and my sister a special thank for your unconditional love and support.

Contents

Introduction	1
1 Sylow p-subgroups of Finite Classical Groups	5
1.1 Sylow Subgroups	6
1.2 Bilinear, Quadratic and Hermitian Forms	7
1.3 Auxiliary Lemmas	12
1.4 A Sylow p -Subgroup for the Unitary Group	17
1.5 A Sylow p -Subgroup for the Symplectic Group	21
1.6 A Sylow p -Subgroup for the Orthogonal Groups	23
2 Invariant Theory	33
2.1 The ring $\mathbb{F}[V]^G$	33
2.2 Properties of the invariant ring $\mathbb{F}[V]^G$	37
2.3 Localisation and Invariant Fields	41
2.4 Constructing Invariants	45
2.4.1 Dickson Invariants	45
2.4.2 Steenrod Operations	49
2.5 <i>SAGBI</i> Bases	50
3 Invariant Fields for Sylow p-subgroups of Finite Classical Groups	58
3.1 Preliminary Results	59

3.2	The Invariant Field of a Sylow p -subgroup of $GU(2m, q^2)$	75
3.3	The Invariant Field of a Sylow p -subgroup of $GU(2m + 1, q^2)$	78
3.4	The Invariant Field of a Sylow p -subgroup of $Sp(2m, q)$	80
3.5	The Invariant Field of a Sylow p -subgroup of $O^+(2m, q)$	82
3.6	The Invariant Field of a Sylow p -subgroup of $O^-(2m + 2, q)$	86
3.7	The Invariant Field of a Sylow p -subgroup of $O(2m + 1, q)$	89
4	Invariant Rings for Sylow p-subgroups of some Finite Classical Groups	91
4.1	The Invariant Ring for a Sylow p -subgroup of $GU(3, q^2)$	92
4.2	The Invariant Ring for a Sylow p -subgroup of $GU(4, q^2)$	98
4.3	The Invariant Ring for a Sylow p -subgroup of $Sp(4, q)$	107
4.4	The Invariant Ring of a Sylow p -subgroup of $O^+(4, q)$, with q odd . . .	113

Introduction

Invariant theory is a subject with a long history in mathematics, motivated by the study of general symmetries in the widest possible sense. Thus, one of the earliest observations in invariant theory is the theorem of symmetric polynomials, expressing the coefficients of a polynomial equation as elementary functions of its roots.

Later a major motivation arose from the natural sciences, in particular physics, where certain configurations are expressed geometrically in terms of numerical functions and coordinates, which may depend on chosen viewpoints and coordinate systems. The change of coordinate systems can then be described by a transformation group, acting on those functions, and the “true, objective” physical entities turn out to be symmetry classes or “orbits” of those functions under the action of the transformation group.

A geometric motivation for studying invariant rings arises in connection with algebraic geometry. If X is an algebraic variety over an algebraically closed field, with a ring of regular functions A , and G is a reductive algebraic group acting on X , then the categorical quotient $X//G$ is isomorphic to $\text{Spec}(A^G)$. Now, if G is a finite group, then $X//G$ is geometric, i.e., $X//G$ is in bijection with the G -orbits of $\text{Spec}(A)$.

The main problem of invariant theory in the nineteenth century was proving the finiteness of the invariant ring. The first results were obtained by Gordan [11] and Hilbert [14]. Gordan in [11] proved that the invariant ring for the special linear group $SL(2, \mathbb{C})$ acting on a symmetric power of the natural representation is finitely generated. In 1890 D. Hilbert in [14] proved this was also true for the general linear group

$GL(n, \mathbb{C})$. Hilbert's first proof was not constructive and involved the "Basissatz" that today is known as the Hilbert Basis Theorem. Later in the beginning of the twentieth century Emmy Noether in [23] proved the finiteness of the invariant ring for finite groups. To solve this problem, Noether introduced the concept of stationary ascending chains of ideals, which we now call the Noetherian condition.

In this thesis we consider finite groups acting on a finite dimensional vector space over a finite field, whose order is divisible by the characteristic of the field. Thus we are working in what is usually called Modular Invariant Theory.

We study the invariant rings for the Sylow p -subgroups of the finite unitary, symplectic and orthogonal groups. Dickson in 1911 proved that the invariant ring $\mathbb{F}_q[V]^{GL(n,q)}$ for the general linear group is a polynomial ring (see [8]). The group of upper triangular matrices with ones along the diagonal is a Sylow p -subgroup of $GL(n, q)$ and its invariant ring is also polynomial (see for example Theorem 3.2 in [6]). Our results, stated in Chapter 4, show that this is not the case for Sylow p -subgroups of general classical groups. This adds more difficulty in getting results in the general case and motivates further investigations.

As a first step in determining presentations for the invariant rings of the Sylow p -subgroups of the finite classical groups, we constructed generators for all the invariant fields. This is an important contribution for the computation of generators and relations for the invariant rings for the Sylow p -subgroups. For example, Carlisle and Kropholler before determining the invariant ring for the symplectic group first constructed the generators for the invariant field.

Although it is known that invariant fields for p -groups are rational and there is even an algorithm to compute its generators (see [4]), it is still quite difficult to apply this algorithm in practice. Also, no bound in the total degree of the generators is given by the algorithm. However, in [10] it was proved that the invariant field for a finite group G is generated by invariants of degree less or equal to $|G|$, i.e., the Noether bound

holds. Our results in Chapter 3 show that the generators for the invariant fields for the Sylow p -subgroups of the finite classical groups have degree much smaller than the order of the group.

We also would like to note that our results about the invariant fields and rings for the Sylow p -subgroups of the finite classical groups, support the conjecture that in all cases invariant rings might be generated by “natural invariants” such as orbit products and Steenrod images of special forms.

The thesis is organised in four chapters. The first two are introductory chapters, although in the first one we used a different approach from what is usually found in the literature. In the last two chapters all the results obtained by us are stated and proved.

The first chapter is used to introduce Sylow p -subgroups of the finite unitary, symplectic and orthogonal groups. Our approach is somehow different from what one might find in the literature. The reason for this is because Sylow p -subgroups are usually studied in the framework of algebraic groups where, using Lie Theory, they appear as roots subgroups, but this does not give us immediately the matrix representations we need.

The second chapter is an introduction to the basic notions and results on invariant theory of finite groups. However, we decided to focus our attention in the properties of the invariant rings that are needed in Chapters 3 and 4. We also would like to stress that the results at end of Section 2.5 on *SAGBI* basis will play an important role in the proofs of our results.

In the third chapter we show how to construct the generators for the invariant fields for the Sylow p -subgroups from Chapter 1. We apply the algorithm from [4], which is described in Section 2.3. The first section of this chapter is technical but its results will simplify the proofs in the subsequent sections.

Finally, in Chapter 4 we construct a generating set and relations for the invariant

rings for the Sylow p -subgroups of the unitary groups $GU(3, q^2)$ and $GU(4, q^2)$, the symplectic group $Sp(4, q)$ and the orthogonal group $O^+(4, q)$ with q odd. In all of them we proved that the invariant ring is a complete intersection and that the generating set is a *SAGBI* basis.

Chapter 1

Sylow p -subgroups of Finite Classical Groups

The purpose of this chapter is to construct Sylow p -subgroups for the finite unitary, symplectic and orthogonal groups. When possible, we construct them as subgroups of the group of lower triangular matrices. Only for some orthogonal groups in even characteristic we will not do this. Nevertheless, for these ones we construct a Sylow p -subgroup generated by a subgroup of lower triangular matrices together with an appropriate element of order two.

We define the classical groups by taking vector spaces over finite fields only. For a more general approach see [27], [1] and [12]. It is known that we can construct these groups in terms of roots subgroups and roots systems through the use of Lie theory. However, an explicit matrix representation is better suited for calculations of polynomial invariants, which is why we choose to construct the Sylow p -subgroups by solving matrix equations. It should be noted that this description cannot be found in the standard literature, such as [27], [1] and [12].

1.1 Sylow Subgroups

In this section we define what a Sylow p -subgroup is and we finish it by stating Sylow's theorem without a proof. It is this theorem that justifies our choice to construct, when possible, the Sylow p -subgroups as subgroups of the group of lower triangular matrices.

Let G be a finite group of order n , i.e, G is a group with n elements. Suppose that $n = p^s m$ where p is a prime number such that p does not divide m .

Definition 1.1 A Sylow p -subgroup of G is a subgroup of order p^s .

A Sylow p -subgroup is an example of the following class of groups.

Definition 1.2 Let p be a prime number. We call H a p -group if its order is a power of p .

We can easily see that a Sylow p -subgroup of G is a maximal p -group contained in G . We write $\text{Syl}_p(G)$ for the set of all Sylow p -subgroups of G .

Theorem 1.3 (Sylow) Let G be a finite group and p a prime divisor of its order. Then:

- (i) The set $\text{Syl}_p(G)$ is non-empty.
- (ii) Any two Sylow p -subgroups H_1 and H_2 are conjugates in G , i.e., $g^{-1}H_1g = H_2$ for some $g \in G$.
- (iii) Every p -subgroup of G is contained in some Sylow p -subgroup of G .

Proof: See Sylow's Theorem in [1], pag. 19. \square

1.2 Bilinear, Quadratic and Hermitian Forms

Throughout this thesis, p will always be a prime number and q a power of p . We denote by \mathbb{F}_q the finite field with q elements. It is well known that \mathbb{F}_q is a finite algebraic extension of \mathbb{Z}_p , the field of integers modulo p . Thus p is the characteristic of \mathbb{F}_q and $a^q = a$ for all a in \mathbb{F}_q .

The finite unitary group is defined in a similar way as it would if we were working with complex numbers. In the finite field case the role of complex conjugation is played by the Frobenius map. To make it more precise we consider an algebraic extension \mathbb{F}_{q^2} of \mathbb{F}_q in degree 2, which is a field with q^2 elements. The Frobenius map $\phi : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ defined by $\phi(a) := a^q$ is then an automorphism of order 2 which leaves the elements of \mathbb{F}_q fixed. For this reason and also for simplicity of notation we write \bar{a} instead of a^q .

Definition 1.4 *Let V be a finite dimensional vector space over \mathbb{F}_{q^2} . An **hermitian form** on V is a map $f : V \times V \longrightarrow \mathbb{F}_{q^2}$ such that*

- (i) $f(u + v, w) = f(u, w) + f(v, w)$ and $f(au, w) = af(u, w)$
- (ii) $f(u, v + w) = f(u, v) + f(u, w)$ and $f(u, aw) = \bar{a}f(u, w)$
- (iii) $f(u, v) = \overline{f(v, u)}$

for all $u, v, w \in V$ and $a \in \mathbb{F}_{q^2}$.

In order to define the symplectic groups we shall need the notion of alternating bilinear forms.

Definition 1.5 *Let V be a finite dimensional vector space over \mathbb{F}_q . The map $f : V \times V \longrightarrow \mathbb{F}_q$ is called a **bilinear form** if it is a linear map in each component, i.e.,*

- (i) $f(u + v, w) = f(u, w) + f(v, w)$ and $f(au, w) = af(u, w)$
- (ii) $f(u, v + w) = f(u, v) + f(u, w)$ and $f(u, aw) = af(u, w)$

for all $u, v, w \in V$ and $a \in \mathbb{F}_q$.

A bilinear form f is called **alternating** if $f(v, v) = 0$ for all $v \in V$, and it is called **symmetric** if $f(u, v) = f(v, u)$ for all $u, v \in V$.

Now, we can say what we mean by a quadratic form on a vector space. Quadratic forms will be used to define the orthogonal groups.

Definition 1.6 A quadratic form on V is a map $Q : V \rightarrow \mathbb{F}_q$ such that

- (i) $Q(av) = a^2Q(v)$ for all $v \in V$ and $a \in \mathbb{F}_q$
- (ii) $f(u, v) := Q(u + v) - Q(u) - Q(v)$ is a bilinear form on V .

The bilinear form f associated to the quadratic form Q is either symmetric or alternating depending on whether the characteristic of \mathbb{F}_q is or is not 2. In the latter case, we can recover Q from f by setting $Q(v) = \frac{1}{2}f(v, v)$ and therefore f and Q are uniquely determined by each other. But in characteristic 2 different quadratic forms can have the same bilinear form.

We are not interested in all possible hermitian, bilinear or quadratic forms on a vector space. We shall restrict ourselves to a special class of them.

Definition 1.7 Let f be a bilinear or an hermitian form on V . Given vectors $u, v \in V$, we say that v is **orthogonal to u** if $f(u, v) = 0$ and in this case we will write $u \perp v$.

If S is a subset of V , then the **orthogonal complement** of S , denoted by S^\perp , is defined by

$$S^\perp := \{v \in V : v \perp s \text{ for all } s \in S\}.$$

The **radical** of V , written $\text{rad}V$, is V^\perp , and f is **non-degenerate** if the radical is zero and **degenerate** otherwise.

A quadratic form Q is said to be non-degenerate (sometimes in the literature this is referred as being non-singular) if the only vector $v \in \text{rad}V$ such that $Q(v) = 0$ is the zero vector.

Note that when the characteristic is not 2 the non-degeneracy of the quadratic form and the bilinear form associated to it are equivalent conditions.

From now on we only consider non-degenerate forms. A vector space V with a non-degenerate alternating bilinear form will be called a symplectic space. If V has a non-degenerate hermitian form, we say that V is a unitary space. Finally, we call V a quadratic space or an orthogonal space if it has a non-degenerate quadratic form on it.

Let $GL(V)$ represent the group of all linear invertible transformations on V . We want to study the elements of $GL(V)$ that preserve the form in any of the above defined spaces.

Definition 1.8 *Let (V, f) be a symplectic or a unitary space. An element σ of $GL(V)$ is called an **isometry** of V if $f(\sigma(u), \sigma(v)) = f(u, v)$ for all $u, v \in V$. In the case of a quadratic space, with a quadratic form Q , we require that $Q(\sigma(v)) = Q(v)$ for all v in V .*

It is easy to check that the set of isometries for a given form is a group. So one could ask if it is possible that two forms of the same type can have the same group of isometries. The answer is yes if they are equivalent.

Definition 1.9 *Let f_1, f_2 be either bilinear or hermitian forms on V . We say that f_1 is **equivalent** to f_2 if there exist $\sigma \in GL(V)$ such that $f_1(u, v) = f_2(\sigma(u), \sigma(v))$ for all $u, v \in V$. And we also say that two quadratic forms Q_1 and Q_2 are equivalent if $Q_1(v) = Q_2(\sigma(v))$ for all $v \in V$.*

By studying the geometric structure introduced by the non-degenerate forms of each type, we can classify them up to equivalence.

Definition 1.10 *Let v be a non-zero vector in V and W, U subspaces of V . Then:*

(i) v is an **isotropic** vector if $f(v, v) = 0$.

(ii) W is a **totally isotropic** subspace if $W \subseteq W^\perp$.

(iii) W is **non-degenerate** if $W \cap W^\perp = 0$.

(iv) We say that V is the **orthogonal direct sum** of U and W if $V = U \oplus W$ and $f(u, w) = 0$ for all $u \in U$ and $w \in W$. In this case we write $V = U \perp W$.

(v) v is a **singular** vector if $Q(v) = 0$.

(vi) W is a **totally singular** subspace if $Q(w) = 0$ for all w in W .

Lemma 1.11 *If W is a non-degenerate subspace of V then $V = W \perp W^\perp$.*

Proof: Let $\{e_1, \dots, e_k\}$ be a basis for W and extend it to a basis $\{e_1, \dots, e_k, e_{k+1}, \dots, e_n\}$ of V . Now, a vector $v = \sum_{j=1}^n v_j e_j$ belongs to W^\perp if and only if

$$0 = f(e_i, v) = \sum_{j=1}^n f(e_i, e_j) v_j, \text{ for all } i \in \{1, \dots, k\}.$$

Define the $k \times n$ matrix $A = [a_{ij}]$ by setting $a_{ij} = f(e_i, e_j)$. Thus $v \in W^\perp$ if and only if v is a solution of the homogeneous system of equations $AX = 0$. Hence $\dim W^\perp \geq n - k$. Since $W \cap W^\perp = 0$ we get

$$\dim(W \oplus W^\perp) = \dim W + \dim W^\perp \geq k + (n - k) = n.$$

Hence $V = W \perp W^\perp$. \square

Definition 1.12 *Let (V, f) be a symplectic or a unitary space. A subspace H of V is called a **hyperbolic plane** if $\dim H = 2$ and H has a basis $\{v, u\}$ such that $f(v, v) = f(u, u) = 0$ and $f(v, u) = 1$. If instead (V, Q) is a quadratic space, then we require $Q(v) = Q(u) = 0$ and $f(v, u) = 1$, where f is the bilinear form associated to Q . We call (u, v) a **hyperbolic pair**.*

It is important to notice that a hyperbolic plane is always non-degenerate. We are going to prove that if V has a non-zero isotropic or singular vector then it contains a hyperbolic plane. The following lemma will be used on its proof.

Lemma 1.13 *Consider the map $\text{Tr} : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_q$ given by $\text{Tr}(\alpha) = \alpha + \bar{\alpha}$. Then Tr is a \mathbb{F}_q -linear map onto \mathbb{F}_q . Moreover, the kernel has dimension 1.*

Proof: See Lemma 10.1 in [27]. \square

Lemma 1.14 *Assume that V is a vector space with a non-degenerate form. If v is an isotropic or singular vector, then there exist a non-zero vector u such that $\{v, u\}$ is a basis of a hyperbolic plane.*

Proof: Let f be hermitian, alternating or the bilinear form associated to a quadratic form Q . The non-degeneracy of the forms guarantee the existence of a non-zero vector u such that $f(v, u) \neq 0$. Furthermore, u can be chosen so that $f(v, u) = 1$.

Note that for any α , $f(v, u - \alpha v) = 1$. Therefore, for each form it is sufficient to show that there exist an α such that $f(u - \alpha v, u - \alpha v) = 0$ or $Q(u - \alpha v) = 0$.

If f is alternating then we can just take α to be zero. For the quadratic form Q choose $\alpha = Q(u)$.

Finally, let f be an hermitian form. Then

$$f(u - \alpha v, u - \alpha v) = f(u, u) - \text{Tr}(\alpha),$$

By Lemma 1.13 there exist an α such that $\text{Tr}(\alpha) = f(u, u)$. This completes the proof. \square

We finish this section with Witt's theorem and its consequences. This is probably one of the most important theorems in the theory of vector spaces with forms. The version of Witt's theorem here included holds for degenerate forms.

Theorem 1.15 (Witt) *Let U be a subspace of V and $\sigma : U \rightarrow V$ an isometry. There is an isometry $\gamma : V \rightarrow V$ such that $\gamma(u) = \sigma(u)$ for all u in U if and only if $\sigma(U \cap \text{rad}V) = \sigma(U) \cap \text{rad}V$.*

Proof: See Theorem 7.4 in [27] \square

There are several consequences of this theorem. First, if V is a symplectic or a unitary space, then all linear isometries of a subspace can be extended to an isometry of V . Also, any two maximal isotropic subspaces of V have the same dimension. The dimension of a maximal isotropic subspace is called **Witt index** of V .

Finally, let V be a quadratic space. Here $\text{rad}V$ can be non trivial. But if U is a totally singular subspace, then an isometry σ of U can be extended to an isometry of V . To see why this follows from Witt's theorem, just note that $\sigma(U)$ will also be a totally singular subspace and $(U + \sigma(U)) \cap \text{rad}V = \{0\}$. Once more, the common dimension of the maximal totally singular subspaces is called the **Witt index** of V .

1.3 Auxiliary Lemmas

The lemmas here presented will play an important role in the construction of the Sylow p -subgroups for each finite classical group.

Let \mathbb{F} be either the finite field \mathbb{F}_q or \mathbb{F}_{q^2} . Define the matrix $\bar{A} := [\bar{a}_{ij}]$ where $\bar{a}_{ij} = a_{ij}^q$.

Notation 1.16 *We represent by $U(n, \mathbb{F})$ the group of $n \times n$ lower triangular matrices with entries in \mathbb{F} and with ones along the diagonal. Also we shall write $M(n \times m, \mathbb{F})$ (or just $M(n, \mathbb{F})$ when $m = n$) for the set of all $n \times m$ matrices whose entries belong to \mathbb{F} . When we want to make clear which field we are working with, we write $U(n, r)$ and $M(n \times m, r)$ (or $M(n, r)$) instead, r being the number of elements in \mathbb{F} .*

Let $X_1, X_3 \in GL(n, \mathbb{F})$ and $X_2 \in M(l, \mathbb{F})$. Consider the following matrix

$$X := \left(\begin{array}{c|c|c} 0 & 0 & X_1 \\ \hline 0 & X_2 & 0 \\ \hline X_3 & 0 & 0 \end{array} \right)$$

in $M(2n + l, \mathbb{F})$. Then the set of all invertible matrices N satisfying $N^T X \bar{N} = X$ is a group and we want to determine its intersection with the group $U(2n + l, \mathbb{F})$.

Let $N \in U(2n + l, \mathbb{F})$ and write it as

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & F & 0 \\ \hline C & D & E \end{array} \right)$$

where $A, E \in U(n, \mathbb{F})$, $F \in U(l, \mathbb{F})$, $C \in M(n, \mathbb{F})$, $B \in M(l \times n, \mathbb{F})$ and $D \in M(n \times l, \mathbb{F})$.

Hence $N^T X \bar{N} = X$ if the system of equations

$$\left\{ \begin{array}{l} A^T X_1 \bar{C} + B^T X_2 \bar{B} + C^T X_3 \bar{A} = 0 \\ A^T X_1 \bar{D} + B^T X_2 \bar{F} = 0 \\ A^T X_1 \bar{E} = X_1 \\ F^T X_2 \bar{B} + D^T X_3 \bar{A} = 0 \\ F^T X_2 \bar{F} = X_2 \\ E^T X_3 \bar{A} = X_3 \end{array} \right. \quad (1.1)$$

is solvable.

If we assume that $X_1^2 = I$, $X_3 = \pm \bar{X}_1^T$ and $\left\{ \begin{array}{ll} X_2 = \bar{X}_2^T & \text{if } X_3 = \bar{X}_1^T \\ X_2 = -\bar{X}_2^T & \text{if } X_3 = -\bar{X}_1^T \end{array} \right.$, then system (1.1) is equivalent to

$$\left\{ \begin{array}{l} D = -\bar{X}_1 (\bar{A}^{-1})^T \bar{B}^T \bar{X}_2 F \\ F^T X_2 \bar{F} = X_2 \\ E = \bar{X}_1 (\bar{A}^{-1})^T \bar{X}_1 \\ C = \bar{X}_1 (\bar{A}^{-1})^T \bar{S} \end{array} \right. \quad (1.2)$$

where $S + \bar{S}^T = -B^T X_2 \bar{B}$ if $X_3 = \bar{X}_1^T$ or $S - \bar{S}^T = -B^T X_2 \bar{B}$ if $X_3 = -\bar{X}_1^T$.

Now, we consider the following subgroups of $U(2n + l, \mathbb{F})$:

- Let $X_3 = \bar{X}_1^T$ and $X_2 = \bar{X}_2^T$. Then we denote by $\mathfrak{G}_{X_1, X_2, X_3}^+$ the group of matrices $N \in U(2n + l, \mathbb{F})$ which satisfy $N^T X \bar{N} = X$.
- Let $X_3 = -\bar{X}_1^T$ and $X_2 = -\bar{X}_2^T$. Then we denote by $\mathfrak{G}_{X_1, X_2, X_3}^-$ the group of matrices $N \in U(2n + l, \mathbb{F})$ which satisfy $N^T X \bar{N} = X$.

In the following lemma we show which elements of $U(2n + l, \mathbb{F})$ belong to each one of the previous groups.

Lemma 1.17 *Let N be an element of $U(2n + l, \mathbb{F})$. Then*

- (i) $N \in \mathfrak{G}_{X_1, X_2, X_3}^+$ if and only if the system (1.2) holds, with $S + \bar{S}^T = -B^T X_2 \bar{B}$.
- (ii) $N \in \mathfrak{G}_{X_1, X_2, X_3}^-$ if and only if the system (1.2) holds, with $S - \bar{S}^T = -B^T X_2 \bar{B}$.

We want to determine the order of $\mathfrak{G}_{X_1, X_2, X_3}^+$ and $\mathfrak{G}_{X_1, X_2, X_3}^-$, when the following assumption holds:

Hypothesis (H): If $\mathbb{F} = \mathbb{F}_q$ with q even, then we assume that the diagonal entries of $B^T X_2 B$ are equal to zero for every $B \in M(l \times n, \mathbb{F})$.

Lemma 1.18 *Under Hypothesis (H), the number of matrices S satisfying:*

$$\begin{aligned}
 (i) \quad S + \bar{S}^T = -B^T X_2 \bar{B} \text{ is } & \begin{cases} q^{n(n-1)} q^n & \text{if } \mathbb{F} = \mathbb{F}_{q^2} \\ q^{\frac{n(n-1)}{2}} & \text{if } \mathbb{F} = \mathbb{F}_q \text{ and } q \text{ odd} \\ q^{\frac{n(n-1)}{2}} q^n & \text{if } \mathbb{F} = \mathbb{F}_q \text{ and } q \text{ even} \end{cases} ; \\
 (ii) \quad S - \bar{S}^T = -B^T X_2 \bar{B} \text{ is } & \begin{cases} q^{n(n-1)} q^n & \text{if } \mathbb{F} = \mathbb{F}_{q^2} \\ q^{\frac{n(n-1)}{2}} q^n & \text{if } \mathbb{F} = \mathbb{F}_q \end{cases} .
 \end{aligned}$$

Proof: We prove (i) and (ii) at the same time. Let $Y := -B^T X_2 \bar{B}$. Then $Y = \bar{Y}^T$ in (i) whereas for (ii), $Y = -\bar{Y}^T$. Hence the number of choices for S in (i) or (ii) is the same as the number of solutions for $M + \bar{M}^T = 0$ or $M - \bar{M}^T = 0$. For both equations the number of solutions only depend on what happens to the diagonal entries of M when we consider different fields. In fact, for the remaining ones the number of possibilities is always $r^{\frac{n(n-1)}{2}}$, where r is the number of elements in \mathbb{F} .

When $\mathbb{F} = \mathbb{F}_q$, a simple argument give us the result. However, if $\mathbb{F} = \mathbb{F}_{q^2}$, then we need to be more careful. Here the equation $M - \bar{M}^T = 0$ implies that $m_{ii} = \bar{m}_{ii}$ for all i . Hence $m_{ii} \in \mathbb{F}_q$ and there are q^n choices for the elements in the diagonal of M . Now, from $M + \bar{M}^T = 0$ we obtain $m_{ii} + \bar{m}_{ii} = 0$, i.e., each m_{ii} belongs to the kernel of the linear map Tr . By Lemma 1.13 there will be q^n different ways of choosing the elements in the diagonal of M . \square

Note that for $\mathfrak{G}_{X_1, X_2, X_3}^+$ and $\mathfrak{G}_{X_1, X_2, X_3}^-$ the number of choices for A and B are the same. If r is the number of elements in \mathbb{F} , then there are $r^{\frac{n(n-1)}{2}}$ choices for A and r^{ln} for B . Let s be number of matrices $F \in U(l, \mathbb{F})$ satisfying $F^T X_2 \bar{F} = X_2$. Applying Lemma 1.18 we obtain the orders of $\mathfrak{G}_{X_1, X_2, X_3}^+$ and $\mathfrak{G}_{X_1, X_2, X_3}^-$.

Lemma 1.19 *Let s be as above. Then:*

$$(i) \text{ The order of } \mathfrak{G}_{X_1, X_2, X_3}^+ \text{ is } \begin{cases} sq^{2n^2+(2l-1)n} & \text{if } \mathbb{F} = \mathbb{F}_{q^2} \\ sq^{n^2+(l-1)n} & \text{if } \mathbb{F} = \mathbb{F}_q \text{ and } q \text{ odd} \\ sq^{n^2+ln} & \text{if } \mathbb{F} = \mathbb{F}_q \text{ and } q \text{ even} \end{cases} ;$$

$$(ii) \text{ The order of } \mathfrak{G}_{X_1, X_2, X_3}^- \text{ is } \begin{cases} sq^{2n^2+(2l-1)n} & \text{if } \mathbb{F} = \mathbb{F}_{q^2} \\ sq^{n^2+ln} & \text{if } \mathbb{F} = \mathbb{F}_q \end{cases} .$$

We finish this section with two technical lemmas. They will be used in Section 1.6 to determine which elements in $\mathfrak{G}_{X_1, X_2, X_3}^+$ preserve the quadratic forms when the characteristic of the field is 2.

Lemma 1.20 For q even and $S \in M(n, q)$ there are unique matrices S' and C , with S' symmetric and C upper triangular, such that $S = S' + C$.

Proof: Define the symmetric matrix $S' = [s'_{ij}]$ by $s'_{ij} = s_{ji}$ for $i \leq j$ and the upper triangular matrix $C := [c_{ij}]$ by

$$c_{ij} = \begin{cases} s_{ij} + s_{ji} & \text{if } i < j \\ 0 & \text{if } i \geq j \end{cases}$$

Then we have $S = S' + C$. The matrices S' and C are unique because $S = S'_1 + C_1 = S'_2 + C_2$ implies that $S'_1 + S'_2 = C_1 + C_2 = 0$. \square

Let J_2 be the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Lemma 1.21 Let $S \in M(n, q)$ and $B \in M(2 \times n, q)$. We also consider the row vectors $X = (\alpha_1, \dots, \alpha_n)$, $Z = (z_1, z_2)$, $Y = (y_1, y_2)$ whose entries belong \mathbb{F}_q . Then

$$(i) \quad XSS^T = \sum_{i=1}^n s_{ii} \alpha_i^2 + \sum_{i=1}^n \sum_{j=1, j \neq i}^n (s_{ij} + s_{ji}) \alpha_i \alpha_j.$$

(ii) If q is even, $S + S^T = B^T J_2 B$ and $Z = Y + XB^T$ then

$$z_1 z_2 = y_1 y_2 + XB^T J_2 Y^T + XCX^T + \sum_{i=1}^n b_{1i} b_{2i} \alpha_i^2$$

where C is the matrix defined in Lemma 1.20.

Proof: The result in (i) is obvious. Let us prove (ii). It is not hard to check that $B^T J_2 B$ is a symmetric matrix and its entries are $b_{1i} b_{2j} + b_{1j} b_{2i}$, $i, j = 1, \dots, n$. From $Z = Y + XB^T$ we get

$$\begin{aligned} z_1 z_2 &= \left(y_1 + \sum_{i=1}^n b_{1i} \alpha_i \right) \left(y_2 + \sum_{j=1}^n b_{2j} \alpha_j \right) \\ &= y_1 y_2 + XB^T J_2 Y^T + \sum_{i=1}^n \sum_{j=1}^n b_{1i} b_{2j} \alpha_i \alpha_j. \end{aligned}$$

Since

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^n b_{1i} b_{2j} \alpha_i \alpha_j &= \sum_{i=1}^n b_{1i} b_{2i} \alpha_i^2 + \sum_{i=1}^n \sum_{j=1, j>i}^n (b_{1i} b_{2j} + b_{1j} b_{2i}) \alpha_i \alpha_j \\ &= \sum_{i=1}^n b_{1i} b_{2i} \alpha_i^2 + X C X^T. \end{aligned}$$

this completes the proof of (ii). \square

1.4 A Sylow p -Subgroup for the Unitary Group

Throughout this section V will be a finite dimensional vector space over a finite field \mathbb{F}_{q^2} and f will be a non-degenerate hermitian form on V . Also, all the matrices and vectors considered will have entries in \mathbb{F}_{q^2} .

We have mentioned in Section 1.2 that the set of isometries for f is a group. We call it the **unitary group** of V and we write it as $GU(V)$. In other words,

$$GU(V) = \{\sigma \in GL(V) : f(\sigma(u), \sigma(v)) = (u, v) \text{ for all } u, v \in V\}.$$

We can look at the elements of the unitary group as being invertible matrices. Let $\{e_1, \dots, e_n\}$ be a basis for V and let $J := [f(e_i, e_j)]$. J is called the matrix of f with respect to the basis $\{e_1, \dots, e_n\}$. If M is the matrix of $\sigma \in GL(V)$ with respect to this basis, then $\sigma \in GU(V)$ if and only if

$$M^T J \bar{M} = J. \tag{1.3}$$

Thus $GU(V)$ is isomorphic to the group $GU(n, q^2)$ of $n \times n$ matrices, with entries in \mathbb{F}_{q^2} , satisfying (1.3).

We shall show that up to isomorphism there is only one unitary group in each dimension. This is the same as saying that all non-degenerate hermitian forms on V are equivalent. This will be the case if for each hermitian form f we can find a basis for V such that f is represented by the same matrix as any other hermitian form.

Define the map $N : \mathbb{F}_{q^2} \setminus \{0\} \rightarrow \mathbb{F}_q \setminus \{0\}$ by $N(a) = a\bar{a}$ for all $a \in \mathbb{F}_{q^2}$. This is a surjective homomorphism (see for example Lemma 10.1 in [27]).

Lemma 1.22 *If $\dim V \geq 2$ then V contains isotropic vectors.*

Proof: First we note that $f(v, v) \in \mathbb{F}_q$. If $v \neq 0$ is not isotropic, then, after possible rescaling, we can assume that $f(v, v) = 1$. Indeed, since the map N is onto we can find an element $a \in \mathbb{F}_{q^2}$ such that $N(a) = f(v, v)^{-1}$ and for $v' = av$ we get $f(v', v') = 1$.

Assume that V does not contain isotropic vectors and pick a non-zero vector v with $f(v, v) = 1$. Lemma 1.11 allow us to choose a non-zero vector u such that $f(v, u) = 0$ and $f(u, u) = 1$. By taking an element $b \in \mathbb{F}_{q^2}$ with $N(b) = -1$ we can easily see that $u + bv$ is isotropic. This contradicts our assumption and the proof is complete. \square

Proposition 1.23 *If V is a unitary space then*

$$V = H_1 \perp H_2 \perp \cdots \perp H_m \perp W$$

where each H_i is a hyperbolic plane and W has dimension 0 or 1. Moreover, if $\dim W = 1$, then W does not contain any isotropic vector and admits a basis w such that $f(w, w) = 1$.

Proof: The proof is done by induction on the dimension of V . If $\dim V = 1$ then $V = W$ and V can not have isotropic vectors because the form is non-degenerate. Now, assume that $\dim V = n > 1$. Applying Lemmas 1.14 and 1.11 we obtain $V = H_1 \perp H_1^\perp$ where H_1 is a hyperbolic plane. We obtain the desired decomposition by induction applied to H_1^\perp . The second part of the proposition is a consequence of the non-degeneracy of the form and the map N being onto. \square

Let $\{u_i, v_i\}$ be a hyperbolic basis for H_i with $i = 1, \dots, m$. Then the subspace generated by the vectors v_1, \dots, v_m is a maximal isotropic subspace and so the Witt

index of V is m . By Witt's theorem V is determined up to isomorphism by m and W . Therefore, all non-degenerate hermitian forms are equivalent.

There is another important consequence of Witt's theorem. If \mathcal{S} is the set of all bases for which the decomposition in Proposition 1.23 holds, then the unitary group $GU(V)$ acts transitively on \mathcal{S} . We determine the order of $GU(V)$ by computing the number of isotropic vectors and hyperbolic basis in V (see [27], pag. 118). If V has dimension n over \mathbb{F}_{q^2} then

$$|GU(V)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - (-1)^i). \quad (1.4)$$

The dimension of W must be 0 or 1 according to Lemma 1.22. We consider the even and the odd dimensional unitary spaces separately.

The following $n \times n$ matrix

$$J_n := \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 1 & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} \quad (1.5)$$

will be repeatedly used throughout the rest of this chapter. Note that $J_n^2 = I$.

Assume that V has even dimension. Then $\dim W = 0$ and by Proposition 1.23 we can choose a basis for V such that the matrix of a non-degenerate hermitian form is

$$J := \left(\begin{array}{c|c|c} 0 & 0 & J_{m-1} \\ \hline 0 & J_2 & 0 \\ \hline J_{m-1} & 0 & 0 \end{array} \right).$$

Therefore, the unitary group $GU(2m, q^2)$ is the group of all invertible matrices M that satisfy (1.3) with J as above.

Proposition 1.24 *Let A be an element in $U(m-1, q^2)$ and $F \in U(2, q^2)$ such that $F^T J_2 \bar{F} = J_2$. Also let B be a $2 \times (m-1)$ matrix, $D = -J_{m-1}(\bar{A}^{-1})^T \bar{B}^T J_2 F$ and S*

is a $(m-1) \times (m-1)$ matrix such that $S + \bar{S}^T = -B^T J_2 \bar{B}$. Then the set G of all matrices of the form

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & F & 0 \\ \hline J_{m-1}(\bar{A}^{-1})^T \bar{S} & D & J_{m-1}(\bar{A}^{-1})^T J_{m-1} \end{array} \right)$$

is a Sylow p -subgroup for the unitary group $GU(2m, q^2)$.

Proof: Applying Lemma 1.17 (i) we can conclude that $G = \mathfrak{G}_{J_{m-1}, J_2, J_{m-1}}^+$.

According to formula (1.4), the Sylow p -subgroup has order q^{2m^2-m} . We show that this is in fact the order of G .

A matrix F satisfies $F^T J_2 \bar{F} = J_2$ if and only if it is of the form $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ with $a + \bar{a} = 0$. Hence there are q different possibilities for F . Applying Lemma 1.19 (i) we obtain that the order of G is equal to q^{2m^2-m} . \square

We are left with the case when $\dim W = 1$. Again, by Proposition 1.23 we can assume that the matrix of the form f is

$$J = \left(\begin{array}{c|c|c} 0 & 0 & J_m \\ \hline 0 & 1 & 0 \\ \hline J_m & 0 & 0 \end{array} \right).$$

According to formula (1.4) a Sylow p -subgroup has order q^{2m^2+m} . The next proposition shows how to choose a Sylow p -subgroup of $GU(2m+1, q^2)$ as a subgroup of $U(2m+1, q^2)$.

Proposition 1.25 *Let A be an element of $U(m, q^2)$, $v \in M(1 \times m, q^2)$, $w = -J_m(\bar{A}^{-1})^T \bar{v}^T$ and S a $m \times m$ matrix such that $S + \bar{S}^T = -v^T \bar{v}$. Then the set G of all matrices of the form*

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline v & 1 & 0 \\ \hline J_m(\bar{A}^{-1})^T \bar{S} & w & J_m(\bar{A}^{-1})^T J_m \end{array} \right)$$

is a Sylow p -subgroup for the unitary group $GU(2m+1, q^2)$.

Proof: If before applying Lemma 1.17 (i) we assume that F is the 1×1 identity matrix, then one can easily show that G is equal to the group $\mathfrak{G}_{J_m, 1, J_m}^+$. Then its order will be q^{2m^2+m} by Lemma 1.19(i) and this completes the proof. \square

1.5 A Sylow p -Subgroup for the Symplectic Group

Let V be a finite dimensional vector space over a finite field \mathbb{F}_q and f a non-degenerate alternating form. The group of isometries of f is called the **symplectic group** of V and we denote it by $Sp(V)$. In other words,

$$Sp(V) = \{\sigma \in GL(V) : f(\sigma(u), \sigma(v)) = (u, v) \text{ for all } u, v \in V\}.$$

Fix a basis $\{e_1, \dots, e_n\}$ for V . Let $J := [f(e_i, e_j)]$ be the matrix of f with respect to this basis. If M is the matrix of $\sigma \in GL(V)$, then $\sigma \in Sp(V)$ if and only if $M^T J M = J$. Hence $Sp(V)$ is isomorphic to the group $Sp(n, q)$.

We shall see that up to isomorphism there is only one symplectic group in each dimension.

Proposition 1.26 *If V is a symplectic space then*

$$V = H_1 \perp H_2 \perp \dots \perp H_m$$

where each H_i is a hyperbolic plane.

Proof: Since the form is alternating, V will always contain isotropic vectors. Now, the result follows by an induction argument as in Proposition 1.23. \square

An immediate consequence of this proposition is that V must have even dimension. Also, the Witt index is m and by Witt's theorem V is determined up to isomorphism by

m . Therefore all alternating forms on V are equivalent because they can be represented by the same matrix.

We say that $\{u_1, \dots, u_m, v_m, \dots, v_1\}$ is a **symplectic basis** if (u_i, v_i) is a hyperbolic pair for $i = 1, \dots, m$. It follows from Witt's theorem that the symplectic group is transitive on the set of all symplectic bases. By counting how many there are, we obtain (see [27], pag. 70):

$$|Sp(2m, q)| = q^{m^2} \prod_{i=1}^m (q^{2i} - 1). \quad (1.6)$$

Consider the matrix $J_h := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then by Proposition 1.26 the matrix of f is

$$J := \left(\begin{array}{c|c|c} 0 & 0 & J_{m-1} \\ \hline 0 & J_h & 0 \\ \hline -J_{m-1} & 0 & 0 \end{array} \right)$$

and M belongs to $Sp(2m, q)$ if and only if $M^T J M = J$.

We construct a Sylow p -subgroup of $Sp(2m, q)$ as being a subgroup of $U(2m, q)$.

Proposition 1.27 *Let A be an element of $U(m-1, q)$ and $F \in U(2, q)$. Let also B be a $2 \times (m-1)$ matrix, $D = -J_{m-1}(A^{-1})^T B^T J_h F$ and S is a $(m-1) \times (m-1)$ matrix such that $S - S^T = -B^T J_h B$. Then the set G of all matrices of the form*

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & F & 0 \\ \hline J_{m-1}(A^{-1})^T S & D & J_{m-1}(A^{-1})^T J_{m-1} \end{array} \right)$$

is a Sylow p -subgroup for the symplectic group $Sp(2m, q)$.

Proof: Apply Lemma 1.17 (ii) to show that $G = \mathfrak{G}_{J_{m-1}, J_h, -J_{m-1}}^-$.

Now, any matrix $F \in U(2, q)$ satisfies $F^T J_h F = J_h$. Hence the number of choices for F is q . Applying Lemma 1.19 (ii) we conclude that G has order q^{m^2} . By formula (1.6) this is the order of a Sylow p -subgroup and the proof is complete. \square

1.6 A Sylow p -Subgroup for the Orthogonal Groups

Throughout this section V will be a finite dimensional vector space over \mathbb{F}_q with a non-degenerate quadratic form Q and f will denote the bilinear form associated to Q . The group of isometries of Q is called the **orthogonal group** of V and we denote it by $O(V)$. In other words,

$$O(V) = \{\sigma \in GL(V) : Q(\sigma(v)) = Q(v) \text{ for all } v \in V\}.$$

If we fix a basis for V , then we can represent each element as an invertible matrix. Hence, $O(V)$ is isomorphic to the group $O(n, q)$.

Remark 1.28 *For any finite field, if an element of $GL(V)$ preserves the quadratic form then it must also preserve the bilinear form. The converse is only true if the field has characteristic not equal to 2.*

Lemma 1.29 *Let $a, b \in \mathbb{F}_q \setminus \{0\}$. Then for all $c \in \mathbb{F}_q$ there exist $x, y \in \mathbb{F}_q$ such that $c = ax^2 + by^2$.*

Proof: See page 138, Lemma 11.1 in [27]. \square

Lemma 1.30 *Let V be a quadratic space with $\dim V \geq 3$. Then V contains a singular vector.*

Proof: See page 138, Theorem 11.2 in [27]. \square

Proposition 1.31 *Let V be a quadratic space. Then there is a basis for V such that*

$$V = H_1 \perp H_2 \perp \cdots \perp H_m \perp W$$

where each H_i is a hyperbolic plane and W does not contain any singular vector. Moreover, the dimension of W is 0, 1 or 2.

Proof: Apply Lemma 1.30 and use induction as in Proposition 1.23. The statement about the dimension of W is a consequence of Lemma 1.30. \square

The number m in the previous proposition is the Witt index and by Witt's theorem V is determined up to isomorphism by m and W .

Since we want to include fields with characteristic 2, we do not classify the quadratic forms by looking at the matrix of the bilinear form associated to it. According to Definition 1.9, we can say that two quadratic forms are equivalent if we can find bases in such a way that they become equal when we write each one of them in terms of the vector components with respect to these bases.

Bearing in mind Proposition 1.31 we make the following important remark. Some claims are not hard to prove and for the less trivial ones, see for example [27], page 139.

Remark 1.32 *Let V be a quadratic space. We have:*

- (i) *If u_i, v_i is a basis for the hyperbolic plane H_i , then $Q(\alpha_i u_i + \beta_i v_i) = \alpha_i \beta_i$.*
- (ii) *If $\dim W = 0$, then there is only one quadratic form and in this case we write $O^+(2m, q)$ for the orthogonal group.*
- (iii) *Assume that $\dim W = 1$ and that w is a basis for W . Then there are two non-equivalent quadratic forms on V depending whether $Q(w)$ is or is not a square in \mathbb{F}_q . However, the orthogonal group is the same for both quadratic forms since we can interchange them by multiplying by a non-square. Therefore we can denote the orthogonal group as $O(2m + 1, q)$.*
- (iv) *Finally, if $\dim W = 2$, then by Lemma 1.29 we can choose a basis w_1, w_2 for W such that $Q(w_1) = 1$ and $f(w_1, w_2) = 1$. Therefore, $Q(\alpha_1 w_1 + \alpha_2 w_2) = \alpha_1^2 + \alpha_1 \alpha_2 + a \alpha_2^2$ where $a = Q(w_2)$ and is such that the polynomial $X^2 + X + a$ is irreducible in $\mathbb{F}_q[X]$. It can be proven that in this case there is only one quadratic*

form in V up to equivalence (see for example [27], page 139). The orthogonal group will then be denoted by $O^-(2m+2, q)$.

The next proposition is a consequence of the previous remark and Proposition 1.31.

Proposition 1.33 *Let V be a quadratic space. Then:*

(i) $O^+(2m, q)$ is the group of invertible matrices preserving the quadratic form

$$Q(v) = \sum_{i=1}^m \alpha_{2m-i+1} \alpha_i.$$

(iii) $O^-(2m+2, q)$ is the group of invertible matrices preserving the quadratic form

$$Q(v) = \sum_{i=1}^m \alpha_{2m+2-i+1} \alpha_i + \alpha_{m+1}^2 + \alpha_{m+1} \alpha_{m+2} + a \alpha_{m+2}^2,$$

where a is such that $X^2 + X + a$ is irreducible in $\mathbb{F}_q[X]$.

(iii) $O(2m+1, q)$ is the group of invertible matrices preserving the quadratic form

$$Q(v) = \sum_{i=1}^m \alpha_{2m+1-i+1} \alpha_i + \alpha_{m+1}^2.$$

Proof: In each case we take the hyperbolic bases u_i, v_i for the hyperbolic planes in Proposition 1.31 and the corresponding bases for W , described in Remark 1.32. Then it is just a matter of writing down the components of v as

$$\begin{aligned} v &= \sum_{i=1}^m (\alpha_i u_i + \alpha_{2m-i+1} v_i) \text{ in (i);} \\ v &= \sum_{i=1}^m (\alpha_i u_i + \alpha_{2m+2-i+1} v_i) + \alpha_{m+1} w_1 + \alpha_{m+2} w_2 \text{ in (ii);} \\ v &= \sum_{i=1}^m (\alpha_i u_i + \alpha_{2m+1-i+1} v_i) + \alpha_{m+1} w \text{ in (iii).} \end{aligned}$$

Now, we apply Remark 1.32 to finish the proof. \square

From now on, we only consider bases like those described in the proof of the previous proposition. The following remark will be useful when constructing a Sylow p -subgroup for the orthogonal groups in characteristic 2. We just rewrite the quadratic forms in a matrix form.

Remark 1.34 Define $X := [\alpha_1 \dots \alpha_m]$ and let J_n be the matrix given by (1.5). Then we can rewrite the quadratic forms associated to each orthogonal group in the following way:

$$(i) \quad Q(v) = X J_{m-1} Y^T + \alpha_{m+1} \alpha_m, \text{ where } Y := [\alpha_{m+2} \dots \alpha_{2m}], \text{ for } O^+(2m, q).$$

$$(ii) \quad Q(v) = X J_m Y^T + \alpha_{m+1}^2 + \alpha_{m+1} \alpha_{m+2} + a \alpha_{m+2}^2, \text{ where } Y := [\alpha_{m+3} \dots \alpha_{2m+2}], \text{ for } O^-(2m+2, q).$$

$$(iii) \quad Q(v) = X J_m Y^T + \alpha_{m+1}^2, \text{ where } Y := [\alpha_{m+2} \dots \alpha_{2m+1}], \text{ for } O(2m+1, q).$$

The order of each orthogonal group is (see [27], pag. 140):

$$|O^+(2m, q)| = 2q^{m(m-1)}(q^m - 1) \prod_{i=1}^{m-1} (q^{2i} - 1); \quad (1.7)$$

$$|O^-(2m+2, q)| = 2q^{m(m+1)}(q^{m+1} + 1) \prod_{i=1}^m (q^{2i} - 1); \quad (1.8)$$

$$|O(2m+1, q)| = \begin{cases} q^{m^2} \prod_{i=1}^m (q^{2i} - 1) & q \text{ even} \\ 2q^{m^2} \prod_{i=1}^m (q^{2i} - 1) & q \text{ odd} \end{cases} \quad (1.9)$$

Now, our goal is to construct a Sylow p -subgroup for each orthogonal group. Bearing in mind remark (1.28) we proceed in the following way. Independently of the characteristic of the field we compute a subgroup G of $U(n, q)$ whose elements preserve the bilinear form f . If q is odd, then G will be a Sylow p -subgroup for $O(n, q)$. However, when q is even not all elements of G will preserve the quadratic form Q . Therefore we determine which ones do and in the process we obtain a subgroup H of G . We will see

that H is a Sylow p -subgroup for $O(n, q)$ with n odd but not for n even. So when n is even we pick an element L in $O(n, q)$ of order 2 which normalises H . Then we show that the subgroup generated by H and L is a Sylow p -subgroup of $O(n, q)$.

We start with the group $O^+(2m, q)$ defined by the quadratic form in Proposition 1.33 (i). Independently of the field, the matrix of the corresponding bilinear form is

$$J := \left(\begin{array}{c|c|c} 0 & 0 & J_{m-1} \\ \hline 0 & J_2 & 0 \\ \hline J_{m-1} & 0 & 0 \end{array} \right).$$

where J_i is given by formula (1.5).

Proposition 1.35 *Let A be an element of $U(m-1, q)$, B a $2 \times m$ matrix and $D = -J_{m-1}(A^{-1})^T B^T J_2$. Also let S a $(m-1) \times (m-1)$ matrix such that $S + S^T = -B^T J_2 B$ and I the 2×2 identity matrix. Then the set G of all matrices of the form*

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & I & 0 \\ \hline J_{m-1}(A^{-1})^T S & D & J_{m-1}(A^{-1})^T J_{m-1} \end{array} \right)$$

is a Sylow p -subgroup for the orthogonal group $O^+(2m, q)$ with q odd.

Proof: Just apply Lemma 1.17 (i) to show that $G = \mathfrak{G}_{J_{m-1}, J_2, J_{m-1}}^+$

The only matrix F satisfying $F^T J_2 F = J_2$ is the identity matrix. Hence, by Lemma 1.19 (i), the order of G is $q^{m(m-1)}$, which according to formula (1.7) is the order of a Sylow p -subgroup for $O^+(2m, q)$ with q odd. \square

Assume that \mathbb{F}_q has characteristic 2 and take G as in the previous proposition. Now, the order of G will be $q^{m(m-1)}q^m$ by Lemma 1.19 (i). We will show that the diagonal entries of the matrices S , in the elements of G that preserve the quadratic form, are not arbitrary. In fact, they will be a function in the entries of B .

Consider the matrix

$$L := \left(\begin{array}{c|c|c} I_{m-1} & 0 & 0 \\ \hline 0 & J_2 & 0 \\ \hline 0 & 0 & I_{m-1} \end{array} \right) \quad (1.10)$$

where I_{m-1} is the identity matrix. Obviously $L \in O^+(2m, q)$ and $L^2 = I$.

Proposition 1.36 *Let G and L be as above. Also, let H be the subset of G such that the matrix S in its elements also satisfy $s_{ii} = b_{1i}b_{2i}$, for $i = 1, \dots, m-1$. Then the elements in G that preserve the quadratic form belong to H and the group G_1 generated by H and L is a Sylow p -subgroup for the orthogonal group $O^+(2m, q)$ with q even.*

Proof: We first determine which elements M in G satisfy $Q(Mv) = Q(v)$. By Remark 1.34 the quadratic form is $Q(v) = XJ_{m-1}Y^T + \alpha_{m+1}\alpha_m$ with $v = [X \ Z \ Y]^T$ and $Z := [\alpha_m \ \alpha_{m+1}]$.

If M is any element of G , then $Mv = [X' \ Z' \ Y']^T$ where

$$\begin{cases} X' = XA^T \\ Z' = Z + XB^T \\ Y' = XS^TA^{-1}J_{m-1} + ZD^T + YJ_{m-1}A^{-1}J_{m-1} \end{cases}$$

Hence,

$$\begin{aligned} Q(Mv) &= X'J_{m-1}(Y')^T + \alpha'_{m+1}\alpha'_m \\ &= XJ_{m-1}Y^T + XSX^T + XB^TJ_2Z^T + \alpha'_{m+1}\alpha'_m. \end{aligned} \quad (1.11)$$

Applying Lemma 1.21 we get

$$XSX^T = \sum_{i=1}^n s_{ii}\alpha_i^2 + XCX^T.$$

$$\alpha'_{m+1}\alpha'_m = \alpha_{m+1}\alpha_m + XB^TJ_2Z^T + XCX^T + \sum_{i=1}^n b_{1i}b_{2i}\alpha_i^2.$$

If we substitute these expressions in (1.11) we obtain

$$Q(Mv) = \sum_{i=1}^m (s_{ii} + b_{1i}b_{2i})\alpha_i^2 + Q(v).$$

Hence M belongs to H . It is not hard to check that all the matrices in H preserve the quadratic form. Therefore H is a subgroup of G with order $q^{m(m-1)}$.

Now, we claim that L normalises the group H . So let $M \in H$. The product $LM L$ only changes the matrices B and D in M to $B' = J_2 B$ and $D' = D J_2$, respectively. A straightforward calculation shows that $S + S^T = (B')^T J_2 B'$ and $D' = -J_{m-1}(A^{-1})^T (B')^T J_2$. Hence $LM L \in H$ and this proves our claim.

The order of G_1 is therefore $2q^{m(m-1)}$ and by formula (1.7) this is the order of a Sylow p -subgroup. This completes the proof. \square

Now, we look at the orthogonal group $O^-(2m+2, q)$. Here the bilinear form associated to the quadratic form in Proposition 1.33 (ii) is going to change when we change from a field of odd characteristic to one of even characteristic. In the former case, the matrix of the bilinear form is

$$J := \left(\begin{array}{c|c|c} 0 & 0 & J_m \\ \hline 0 & J_a & 0 \\ \hline J_m & 0 & 0 \end{array} \right)$$

$$\text{where } J_a := \begin{pmatrix} 2 & 1 \\ 1 & 2a \end{pmatrix}.$$

Proposition 1.37 *Let A be an element of $U(m, q)$, B a $2 \times m$ matrix and $D = -J_m(A^{-1})^T B^T J_a$. Also let S be a $m \times m$ matrix such that $S + S^T = -B^T J_a B$ and I the 2×2 identity matrix. Then the set G of all matrices of the form*

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & I & 0 \\ \hline J_m(A^{-1})^T S & D & J_m(A^{-1})^T J_m \end{array} \right)$$

is a Sylow p -subgroup for the orthogonal group $O^-(2m+2, q)$ with q odd.

Proof: First, we note that if $F \in U(2, q)$ is a solution for the matrix equation $F^T J_a F = J_a$, then F must be the identity matrix.

From Lemma 1.17 (i) it follows that $G = \mathfrak{G}_{J_{m-1}, J_a, J_{m-1}}^+$ and by Lemma 1.19 (i) its order is $q^{m(m+1)}$. Since this order is equal to the one given by formula (1.8) we conclude that G is a Sylow p -subgroup $O^-(2m+2, q)$ for q odd. \square

Let us consider the group $O^-(2m+2, q)$ with q even. The matrix of the bilinear form f associated to the quadratic form in Proposition 1.33 (ii) is the same as the one for the group $O^+(2(m+1), q)$. Therefore we consider the group G in Proposition 1.35 with m replaced by $m+1$. Its elements also preserve the bilinear form f and G has order $q^{m(m+1)}q^m$. Similar to what we have done for $O^+(2m, q)$, with q even, we shall prove that the elements in G that preserve the quadratic form, their corresponding matrices S do not have arbitrary diagonal entries.

If in (1.10) we replace m by $m+1$ and the matrix J_2 by $J'_2 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ we obtain an element L_1 in $O^-(2m+2, q)$ of order 2. In fact, we know from Remark 1.34 that

$$Q(v) = XJ_m Y^T + \alpha_{m+1}^2 + \alpha_{m+1}\alpha_{m+2} + a\alpha_{m+2}^2$$

with $v = [X \quad \alpha_{m+1} \quad \alpha_{m+2} \quad Y]^T$. Now, it is not hard to see that $L_1 v = [X \quad \alpha_{m+1} + \alpha_{m+2} \quad \alpha_{m+2} \quad Y]^T$ and therefore $Q(L_1 v) = Q(v)$.

Proposition 1.38 *Let G and L_1 be as above. We consider the subset H of G by adding the extra condition $s_{ii} = b_{1i}^2 + b_{1i}b_{2i} + ab_{2i}^2$, for $i = 1, \dots, m$, to S . Then the group G_1 generated by H and L_1 is a Sylow p -subgroup for the orthogonal group $O^-(2m+2, q)$ with q even.*

Proof: Once more we make use of Remark 1.34. Therefore we write the quadratic form as $Q(v) = XJ_m Y^T + \alpha_{m+1}^2 + \alpha_{m+1}\alpha_{m+2} + a\alpha_{m+2}^2$ with $v = [X \quad Z \quad Y]^T$ and $Z := [\alpha_{m+1} \quad \alpha_{m+2}]$. In a similar way to what was done in the proof of Proposition 1.36,

we get for an element M in G that

$$Q(Mv) = \sum_{i=1}^m (s_{ii} + b_{1i}^2 + b_{1i}b_{2i} + ab_{2i}^2)\alpha_i^2 + Q(v)$$

and therefore M preserves the quadratic form if and only if M is an element of H . Thus H is subgroup of G with order $q^{m(m+1)}$.

To prove that L_1 normalises H just repeat the same argument as in Proposition 1.36 and use the fact that $(J'_2)^T J_2 J'_2 = J_2$.

Hence G_1 has order $2q^{m(m+1)}$ which is actually the order of a Sylow p -subgroup for $O^-(2m+2, q)$ with q even (see formula (1.8)). \square

Finally, we construct Sylow p -subgroups for the orthogonal groups $O(2m+1, q)$. They will always be a subgroup $U(2m+1, q)$ independently of which field we take.

First, assume that \mathbb{F}_q is a field with odd characteristic. Then the matrix of the bilinear form associated to the quadratic form in Proposition 1.33 (iii) is

$$J := \left(\begin{array}{c|c|c} 0 & 0 & J_m \\ \hline 0 & 2 & 0 \\ \hline J_m & 0 & 0 \end{array} \right).$$

If we apply Lemma 1.17 (i) then we obtain a subgroup of $U(2m+1, q)$ whose elements satisfy $M^T J M = J$.

Proposition 1.39 *Let A be an element of $U(m, q)$, $v \in M(1 \times m, q)$, $w = -J_m(A^{-1})^T v^T$ and S a $m \times m$ matrix such that $S + S^T = -2v^T v$. Then the set G of all matrices of the form*

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline v & 1 & 0 \\ \hline J_m(A^{-1})^T S & w & J_m(A^{-1})^T J_m \end{array} \right)$$

is a Sylow p -subgroup for the orthogonal group $O(2m+1, q)$ with q odd.

Proof: By taking F as the 1×1 identity matrix it follows from Lemma 1.17 (i) that $G = \mathfrak{G}_{J_m, 2, J_m}^+$. Applying Lemma 1.19 (i) we conclude that the order of G is q^{m^2}

and from formula (1.9) we can see that this is the order of a Sylow p -subgroup of $O(2m+1, q)$ for q odd. This proves the proposition. \square

Now, assume that \mathbb{F}_q has even characteristic. Then the matrix of the bilinear form is

$$J := \left(\begin{array}{c|c|c} 0 & 0 & J_m \\ \hline 0 & 0 & 0 \\ \hline J_m & 0 & 0 \end{array} \right).$$

Proposition 1.40 *Let A be an element of $U(m, q)$, $v \in M(1 \times m, q)$. Also let S a $m \times m$ matrix such that $S + S^T = 0$ and $s_{ii} = v_i^2$ for $i = 1, \dots, m$. Then the set H of all matrices of the form*

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline v & 1 & 0 \\ \hline J_m(A^{-1})^T S & 0 & J_m(A^{-1})^T J_m \end{array} \right) \quad (1.12)$$

is a Sylow p -subgroup for the orthogonal group $O(2m+1, q)$ with q even.

Proof: First we determine the elements of $U(2m+1, q)$ that preserve the bilinear form. Applying Lemma 1.17 (i) and assuming from the start that F is the 1×1 identity matrix, we obtain the group $G := \mathfrak{G}_{J_m, 0, J_m}^+$ whose matrices are of the form (1.12), with $S + S^T = 0$. Hence, by Lemma 1.19 (i), G has order $q^{m^2} q^m$.

Remark 1.34 shows that $Q(v) = X J_m Y^T + \alpha_{m+1}^2$ with $v = [X \ \alpha_{m+1} \ Y]^T$. Applying the same steps as in the proof of Proposition 1.36, we obtain for an element M in G that

$$Q(Mv) = \sum_{i=1}^m (s_{ii} + v_{ii}^2) \alpha_i^2 + Q(v).$$

Hence M preserves the quadratic form if and only if M belongs to H . From this we can conclude that H is a subgroup of order q^{m^2} , which implies that H is a Sylow p -subgroup for $O(2m+1, q)$ with q even (see formula (1.9)). \square

Chapter 2

Invariant Theory

The aim of this chapter is to give an introduction to the Invariant Theory of Finite Groups. We will focus our attention to the results and concepts which will be used later on in Chapters 3 and 4. Of particular interest is the last section on *SABGI* bases, whose results will play an important role in the construction of generators for the invariant rings in Chapter 4.

2.1 The ring $\mathbb{F}[V]^G$

Let V be a finite dimensional vector space over a field \mathbb{F} . We denote by $\mathbb{F}[V]$ the symmetric algebra of V^* , the dual space of V consisting of all linear maps from V to \mathbb{F} . If V has dimension n and $\{x_1, \dots, x_n\}$ is a basis for V^* then

$$\mathbb{F}[V] = \mathbb{F} \oplus V^* \oplus S^2(V^*) \oplus S^3(V^*) \oplus \dots$$

where $S^m(V^*)$ is the m -th symmetric power of V^* . Its elements are homogeneous polynomials of degree m in x_1, \dots, x_n . Thus $S^m(V^*)$ is a vector space over \mathbb{F} with basis $\{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} : i_1 + i_2 + \cdots + i_n = m\}$ and $\mathbb{F}[V]$ is isomorphic to the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$.

Definition 2.1 *Let G be a finite group and V a vector space over a field \mathbb{F} . A **linear representation** of G is an homomorphism of groups*

$$\rho : G \longrightarrow GL(V).$$

A linear representation induces a left action of G on V by

$$\sigma.v = \rho(\sigma)(v)$$

for all v in V and all g in G . This action can be extended to $\mathbb{F}[V]$. Since we want a linear action on $\mathbb{F}[V]$, it is enough to show how G acts on V^* and on $S^m(V^*)$. In each case we define the G -action on a basis and then we extend it linearly to the entire space. Let $\{x_1, \dots, x_n\}$ be a basis of V^* . Then we define an action:

- on V^* by $(\sigma.x_i)(v) := x_i((\rho(\sigma)^{-1})(v))$ for all v in V and all g in G ;
- on $S^m(V^*)$ by $\sigma.(x_1^{i_1}x_2^{i_2} \cdots x_n^{i_n}) := (\sigma.x_1)^{i_1}(\sigma.x_2)^{i_2} \cdots (\sigma.x_n)^{i_n}$, where $i_1 + i_2 + \cdots + i_n = m$.

Thus, we get a left linear action on $\mathbb{F}[V]$. In other words, G acts on the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$ by linear substitutions of x_1, \dots, x_n . Moreover, we can easily see that the action is degree preserving, i.e., if $f \in \mathbb{F}[V]$ is an homogeneous polynomial of degree d , then $\sigma.f$ is also homogeneous of the same degree.

Remark 2.2 *If $\sigma \in G$ is represented by a matrix A in $GL(V)$ with respect to a fixed basis then the matrix of σ with respect to the dual basis is $(A^{-1})^T$. By considering left matrix multiplication on column vectors, σ acts on V and on V^* via A and $(A^{-1})^T$, respectively. We take the inverse of the matrix A^T in order to obtain a left action rather than a right action on V^* . This is not an issue when we want to compute the orbit of an element in V^* . Also, in order to avoid having to compute A^{-1} we just write down the matrix A meaning that the action on V^* is given by A^T and on V by A^{-1} .*

The basic object of study in invariant theory is the set of polynomials in $\mathbb{F}[V]$ which are left fixed by all elements in G . This set is a ring, called the **invariant ring** for G , and it will be denoted by $\mathbb{F}[V]^G$. Hence

$$\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid \sigma.f = f \quad \forall \sigma \in G\}.$$

It is customary in Invariant Theory of Finite Groups to distinguish the cases when the order of the group is divisible by the characteristic of the field and when it is not. The former we call the non-modular case and the latter the modular case.

A classical example is the ring of invariants for the symmetric group.

Example 2.3 *Let Σ_3 be the symmetric group in 3 letters which acts on $\mathbb{F}[x_1, x_2, x_3]$ by permuting the variables x_1, x_2, x_3 . The elementary symmetric functions are*

$$s_1 = x_1 + x_2 + x_3, \quad s_2 = x_1x_2 + x_1x_3 + x_2x_3, \quad s_3 = x_1x_2x_3.$$

Then the invariant ring for Σ_3 is generated by s_1, s_2, s_3 (see [25], Theorem 1.1.1), i.e.,

$$\mathbb{F}[V]^{\Sigma_3} = \mathbb{F}[s_1, s_2, s_3].$$

This means that every element in $\mathbb{F}[V]^{\Sigma_3}$ is written as a polynomial in s_1, s_2, s_3 with coefficients in \mathbb{F} .

The previous example shows that the invariant ring was finitely generated. However, not all groups have finitely generated rings of invariants. The first example of such groups was given by Nagata in [20]. In Section 2.2, we will show that for finite groups the invariant ring is always finitely generated, a result that was obtained by Emmy Noether in [23]. In general, the ring of invariants will be finitely generated if G is a reductive algebraic group. The question about the finiteness of the invariant ring started in the 19th century with the works of Gordan [11] and Hilbert [14]. Gordan in [11] proved that the invariant ring for the special linear group $SL(2, \mathbb{C})$ acting on a symmetric power of the natural representation is finitely generated. In 1890 D. Hilbert

in [14] proved this was also true for the general linear group $GL(n, \mathbb{C})$. Weyl in [28] proved the finiteness of $\mathbb{C}[V]^G$ for any reductive group G . For an arbitrary field, Nagata in [21] proved the finite generation of $\mathbb{F}[V]^G$ if G is a geometrically reductive group. Later Haboush in [13] showed that reductive groups are geometrically reductive.

Another aspect of Invariant Theory of Finite Groups is related to the structure of the invariant ring. For example, the invariant ring for the symmetric group Σ_3 in Example 2.3 is a polynomial ring. The next example shows that this is not always the case.

Example 2.4 *Let $G := \langle g \rangle$ be the cyclic group of order 2 and \mathbb{F} a field of characteristic different from 2. We define a G -action on $\mathbb{F}[x_1, x_2]$ by*

$$gx_1 = -x_1 \quad \text{and} \quad gx_2 = -x_2.$$

Then it is not hard to prove that $\mathbb{F}[x_1, x_2]^G = \mathbb{F}[x_1^2, x_2^2, x_1x_2]$. The polynomials x_1^2, x_2^2 and x_1x_2 are irreducibles in $\mathbb{F}[x_1, x_2]^G$ and the two non-associate factorisations $x_1^2x_2^2 = (x_1x_2)^2$ show that $\mathbb{F}[x_1, x_2]^G$ is not a unique factorization domain.

The following theorem is a useful criterion to check if an invariant ring for a finite group is a polynomial ring.

Theorem 2.5 *Let $f_1, \dots, f_n \in \mathbb{F}[V]^G$ be homogeneous invariants with $n = \dim V$. Then the following statements are equivalent:*

- (i) $\mathbb{F}[V]^G = \mathbb{F}[f_1, \dots, f_n]$.
- (ii) *The f_i are algebraically independent over \mathbb{F} and $\prod_{i=1}^n \deg(f_i) = |G|$.*

Proof: See Proposition 16 in [16] or Theorem 3.7.5 in [7]. \square

In the non-modular case, it is known that the invariant ring $\mathbb{F}[V]^G$ is a polynomial ring if and only if the representation of G is generated by pseudo-reflections, i.e., by

non-identity elements of finite order which leave a hyperplane fixed pointwise. This is the famous Shephard-Todd-Chevalley theorem. However, in the modular case, classifying the representations of groups who have a polynomial invariant ring is not complete. Nakajima [22] classified all p -groups over the prime field \mathbb{F}_p which have polynomial invariant rings. These groups are known as Nakajima groups. In a larger field Nakajima's result is not true. Finally, Kemper and Malle in [18] have classified the finite groups G with an irreducible representation for which the $\mathbb{F}[V]^G$ is a polynomial ring.

2.2 Properties of the invariant ring $\mathbb{F}[V]^G$

In this section we shall see that the invariant ring for finite groups is finitely generated and always contains a homogeneous system of parameters. First, we need some notions from commutative algebra.

Let A be a commutative ring with identity. An A -module M is defined by the same axioms as is a vector space over a field, but with the field elements being replaced by elements in A . It is a generalisation of the concept of vector space. So familiar notions of linear algebra like linear combinations, generating subsets, linearly independent elements, subspaces, linear homomorphisms and many others, are defined in the same way for an A -module. We just replace the usual scalars by the elements of A . However, some properties of vector spaces do not hold for modules. For example, not all A -modules have bases.

We say that a module M over a commutative ring A is **Noetherian** if every ascending chains of submodules eventually becomes stationary. The ring A is said to be Noetherian if it is so as a module over itself.

Proposition 2.6 *Let M be an A -module. Then M is Noetherian if and only if every submodule of M is finitely generated.*

Proof: See Proposition 6.2 of [2]. \square

Let $B \subseteq A$ be an extension of commutative rings with the same identity. Then we say that A is an **algebra** over B . In particular, A is a B -module. We say that A is finitely generated as a B -algebra if there is a finite number of elements a_1, \dots, a_m in A such that every element of A is expressible as a polynomial in a_1, \dots, a_m with coefficients in B or, equivalently, there is B -algebra homomorphism from a polynomial ring $B[X_1, \dots, X_m]$ onto A . For example, the polynomial ring $\mathbb{F}[V]$ is a finitely generated \mathbb{F} -algebra.

Remark 2.7 *It follows from the Hilbert Basis Theorem that every finitely generated \mathbb{F} -algebra is a Noetherian ring. In particular, the polynomial ring $\mathbb{F}[V]$ is Noetherian.*

Proposition 2.8 *Let A be a Noetherian ring and M a finitely generated A -module. Then M is Noetherian.*

Proof: See Proposition 6.5 of [2]. \square

Definition 2.9 *Let $B \subseteq A$ be an extension of commutative rings. Then*

- *An element $a \in A$ is **integral** over B if it is a root of a monic polynomial with coefficients in B ;*
- *We say that A is **integral** over B if every element of A is integral over B .*
- *B is said to be **integrally closed** in A if every element in A integral over B belongs to B .*

Proposition 2.10 *Let A be a finitely generated B -algebra. Then A is integral over B if and only if A is finitely generated as a B -module.*

Proof: See proposition 5.1.1 in [25]. \square

Theorem 2.11 (Emmy Noether) *Let G be a finite group acting on a commutative finitely generated \mathbb{F} -algebra A by algebra automorphisms. Then A is integral over A^G and A^G is a finitely generated \mathbb{F} -algebra.*

Proof: Let x_1, x_2, \dots, x_m be generators for A . The polynomials

$$\prod_{\sigma \in G} (X - \sigma x_i) = X^m + a_{i,1}X^{m-1} + \dots + a_{i,m-1}X + a_{i,m} \in A^G[X]$$

provide an integral equation for each x_i over A^G . This proves that A is integral over A^G .

If we define B to be the subalgebra of A^G generated by the coefficients $a_{i,j}$ of the monic polynomials satisfied by each generator x_i , then A is also integral over B . By Proposition 2.10 A is a finitely generated B -module. From the Hilbert Basis theorem we conclude that B is Noetherian and applying Proposition 2.8 we get that A is a Noetherian B -module. Since A^G is a B -submodule of A , it follows from Proposition 2.6 that A^G is a finitely generated B -module. In particular, A^G is a finitely generated \mathbb{F} -algebra. \square

The previous theorem shows that $\mathbb{F}[V]^G$ is a finitely generated \mathbb{F} -algebra. But its proof does not provide us with a procedure to find the generators for the invariant ring. Nevertheless, it shows that when constructing a finitely generated subalgebra A of $\mathbb{F}[V]^G$, we must have $\mathbb{F}[V]$ integral over A if we are to prove that A is equal to $\mathbb{F}[V]^G$. This is not too hard to achieve. It follows from another property of $\mathbb{F}[V]^G$: the existence of a homogeneous system of parameters.

Definition 2.12 *A graded algebra is an algebra A together with a family $(A_n)_{n \geq 0}$ of \mathbb{F} -vector spaces such that $A_0 = \mathbb{F}$ and*

$$A = \bigoplus_{n \geq 0} A_n$$

with $A_n A_m \subset A_{n+m}$ for all n and m .

Since we can write $\mathbb{F}[V]$ as

$$\mathbb{F}[V] = \bigoplus_{d \geq 0} \mathbb{F}[V]_d$$

where $\mathbb{F}[V]_d$ is the subspace formed by the homogeneous polynomials of degree d , it follows that $\mathbb{F}[V]$ is a graded algebra. The G -action on $\mathbb{F}[V]$ is degree preserving and so $\mathbb{F}[V]^G$ is also a graded algebra with decomposition

$$\mathbb{F}[V]^G = \bigoplus_{d \geq 0} \mathbb{F}[V]_d^G.$$

Definition 2.13 Suppose that $A = \bigoplus_{d=0}^{+\infty} A_d$ is a graded algebra over a field \mathbb{F} such that $A_0 = \mathbb{F}$. A set $\{f_1, \dots, f_n\} \subset A$ of homogeneous elements is called a **homogeneous system of parameters** if

- (i) f_1, \dots, f_n are algebraically independent and
- (ii) A is a finitely generated module over $\mathbb{F}[f_1, \dots, f_n]$.

It follows from the Noether Normalisation Lemma that homogeneous system of parameters always exist for invariant rings (see for example [25], Chapter 5, Section 5.3).

To check whether a set of invariant polynomials is a homogeneous system of parameters we will use the next lemma. First, we introduce some notation. Let $\bar{\mathbb{F}}$ be the algebraic closure of \mathbb{F} and let $\bar{V} := \bar{\mathbb{F}} \otimes_{\mathbb{F}} V$. Given a set of polynomials S in $\mathbb{F}[V]$ we define the variety $\mathcal{V}_{\bar{\mathbb{F}}}(S)$ by

$$\mathcal{V}_{\bar{\mathbb{F}}}(S) := \{v \in \bar{V} \mid f(v) = 0 \text{ for all } f \in S\}.$$

Lemma 2.14 Let $S = \{h_1, \dots, h_n\}$ be a set of homogeneous elements of $\mathbb{F}[V]^G$ with $n = \dim V$. Then S is a homogeneous system of parameters for $\mathbb{F}[V]^G$ if and only if $\mathcal{V}_{\bar{\mathbb{F}}}(S) = \{0\}$.

Proof: See Proposition 3.3.1 of [7]. \square

We introduce the Krull dimension of a commutative ring.

Definition 2.15 The **Krull dimension** of a commutative ring A , written $\dim A$, is the maximum length k of chains of proper prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_k \subsetneq A$. If \mathfrak{p} is a prime ideal in A , then we define the **height** of \mathfrak{p} to be the maximum length l of proper chains of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_l = \mathfrak{p}$ ending at \mathfrak{p} .

Proposition 2.16 The Krull dimension of $\mathbb{F}[V]$ is equal to $\dim V$.

Proof: See Proposition 5.2.2 of [25]. \square

Corollary 2.17 The Krull dimension of the invariant ring $\mathbb{F}[V]^G$ is also equal to $\dim V$.

Proof: Since $\mathbb{F}[V]$ is integral over $\mathbb{F}[V]^G$, this is an immediate consequence of Proposition 9.2 in [9]. \square

Definition 2.18 A sequence of elements a_1, \dots, a_n in a ring A is called a **regular sequence** if the ideal (a_1, \dots, a_n) generated by them is proper and for each i the image of a_{i+1} is not a zero divisor in $A/(a_1, \dots, a_i)$.

Definition 2.19 A \mathbb{F} -algebra A is called a **complete intersection** if it is isomorphic to a quotient ring

$$\mathbb{F}[X_1, \dots, X_{n+m}]/(R_1, \dots, R_m)$$

where $n = \dim A$ and $m \geq 0$.

We will see that all the invariant rings computed in Chapter 4 are complete intersections.

2.3 Localisation and Invariant Fields

Let A be a ring with identity and $S \subset A \setminus \{0\}$ a subset which is closed under multiplication and contains the identity 1. The **localisation** of A with respect to S , denoted

by $S^{-1}A$, is the ring of formal fractions

$$S^{-1}A = \left\{ \frac{a}{s} : a \in A, s \in S \right\}$$

where two such fractions $\frac{a}{s}$ and $\frac{a'}{s'}$ are considered equal if and only if there exist $u \in S$ such that

$$(as' - a's)u = 0.$$

Two important examples of this construction will be used in this thesis:

- When $S := \{a^m : m \geq 0\}$ for some $a \in A \setminus \{0\}$. In this case we write $A[a^{-1}]$ for $S^{-1}A$.
- When A is an integral domain and $S = A \setminus \{0\}$. Then the localisation of A at S is the field of fractions of A which we denote by $\text{Quot}(A)$ instead of $S^{-1}A$.

Let $\mathbb{F}(V)$ denote the field of fractions of $\mathbb{F}[V]$. We extend the action of G on $\mathbb{F}[V]$ to its field of fractions by

$$g(f_1/f_2) := g(f_1)/g(f_2).$$

The elements of $\mathbb{F}(V)$ which are left fixed by all elements of G is a field, called the **Invariant Field** which we denote by $\mathbb{F}(V)^G$.

Proposition 2.20 *Suppose that V is a finite dimensional faithful representation of a finite group G over a field \mathbb{F} . Then $\mathbb{F}(V)$ is a Galois (i.e., normal and separable) extension of $\mathbb{F}(V)^G$ with Galois group G . The field $\mathbb{F}(V)^G$ is the field of fractions of $\mathbb{F}[V]^G$, and $\mathbb{F}[V]^G$ is integrally closed in $\mathbb{F}(V)^G$.*

Proof: See proposition 1.1.1 of [3]. \square

Remark 2.21 *It follows from Galois theory that if H is a normal subgroup of G then*

$$\mathbb{F}(V)^G \subset \mathbb{F}(V)^H$$

is a Galois extension with Galois group G/H . This means that $\mathbb{F}(V)^G$ is the fixed field of $\mathbb{F}(V)^H$ under the action of G/H , i.e.,

$$\mathbb{F}(V)^G = (\mathbb{F}(V)^H)^{G/H}.$$

From the previous proposition we can establish a strategy to find the invariant ring for a finite group G acting on a finite dimensional vector space V . First, we choose a finite set of homogeneous invariant polynomials and we consider the algebra A generated by this set. Then A is equal to $\mathbb{F}[V]^G$ if we can prove that

- $\mathbb{F}[V]$ is integral over A . This can be easily achieved if A contains a homogeneous system of parameters for the invariant ring.
- The field of fractions of A is the same as the one for $\mathbb{F}[V]^G$. In this section we describe a method which is used in Chapter 3 to check this.
- A is integrally closed in $\text{Quot}(A)$. This is the hardest step to prove. In the end of this section we state a lemma which will be applied several times in Chapter 4.

All the groups that we are interested in studying their invariant rings are p -groups. It is known that for p -groups the invariant field $\mathbb{F}(V)^G$ is purely transcendental over \mathbb{F} (see [19]).

The next lemma is useful tool to check if a certain set of invariant homogeneous polynomials are a generating set for the invariant field or not.

Lemma 2.22 *Let $f_1, \dots, f_n \in \mathbb{F}[V]^G$, with $n = \dim V$, be homogeneous invariants such that the Jacobian determinant $\det \left(\frac{\partial f_i}{\partial f_j} \right)$ is non-zero and*

$$\prod_{i=1}^n \deg(f_i) < 2|G|.$$

Then $\mathbb{F}(V)^G = \mathbb{F}(f_1, \dots, f_n)$.

Proof: It follows from Corollary 1.8 in [17]. \square

However, we can have $n = \dim V$ invariants polynomials that generate $\mathbb{F}(V)^G$ but the product of their degrees is equal to or greater than $2|G|$. Hence, the previous lemma fails to detect such generating sets. For p -groups it turns out that we can construct a generating set for invariant field algorithmically. This is due to Campbell & Chuai [4] and Kang [5]. We now present the algorithm as it is described in [4].

Let G be a p -group. Since any p -subgroup of $GL(V)$ is triangularizable, there exist a basis e_1, \dots, e_n for V such that each element of G (more precisely, each element of $\rho(G)$ where ρ is a linear representation of G) is represented by a lower triangular matrix with ones along the diagonal. Therefore if x_1, \dots, x_n is the dual basis with respect to e_1, \dots, e_n , then $(\sigma - 1)x_m$ is in the subspace spanned by x_1, \dots, x_{m-1} for all $\sigma \in G$. From this we can easily see that x_1 is invariant.

We define $R[j] := \mathbb{F}[x_1, \dots, x_j]$ for $0 \leq j \leq n$ subject to the convention that $R[0] := \mathbb{F}$. Then G acts on each ring $R[j]$. For each j we choose an invariant $\phi_j \in R[j]^G$ with the smallest positive degree in x_j among the elements of $R[j]^G$.

Theorem 2.23 *Let G be a p -group. Then the polynomials ϕ_1, \dots, ϕ_n above defined generate the invariant field for G , i.e.,*

$$\mathbb{F}(V)^G = \mathbb{F}(\phi_1, \dots, \phi_n).$$

Moreover, there exists $f \in \mathbb{F}[\phi_1, \dots, \phi_n]$ such that

$$\mathbb{F}[V]^G[f^{-1}] = \mathbb{F}[\phi_1, \dots, \phi_n][f^{-1}].$$

Proof: See Theorem 2.4 in [4]. \square

Now, we are left with how to show that our test algebra A is integrally closed. This can be done by applying the following lemma:

Lemma 2.24 *Suppose that A is a Noetherian integral domain. If $x_1 \in A$ is prime and $A[x_1^{-1}]$ is a unique factorization domain, then A is also a unique factorization domain.*

Proof: See Proposition 6.3.1 of [3]. \square

2.4 Constructing Invariants

In this section we describe a few methods to construct invariant polynomials.

Let G be a finite group acting on the polynomial ring $\mathbb{F}[V]$ as described in Section 2.1. For an element $f \in \mathbb{F}[V]$, we define the **orbit** of f under the G -action, denoted by Gf , to be

$$Gf := \{\sigma f : \sigma \in G\}.$$

If we take the product of all elements in Gf we clearly obtain an invariant polynomial. This is called the **orbit product** of f which we denote by $N(f)$, i.e.,

$$N(f) := \prod_{g \in Gf} g.$$

Another way to construct an invariant polynomial from f would be to take the sum of all elements σf with $\sigma \in G$. This is called the **transfer or trace** of f and we write it as $\text{Tr}(f)$, i.e.,

$$\text{Tr}(f) := \sum_{\sigma \in G} \sigma f.$$

2.4.1 Dickson Invariants

Let \mathbb{K} be a field containing a n -dimensional vector space V over the finite field \mathbb{F}_q , where $q = p^m$. Also, let G be the group of automorphisms of V , i.e., $G = GL(V)$. Dickson in 1911 proved that the invariant ring $\mathbb{F}_q[V]^G$ is the polynomial ring $\mathbb{F}_q[c_0, \dots, c_{n-1}]$ on generators c_i of degree $q^n - q^i$ (see [8]).

The homogeneous polynomials c_i , $i = 0, \dots, n-1$, can be defined as the coefficients of the polynomial

$$F_{n,q}(X) := \prod_{u \in V^*} (X - u) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_i X^{q^i} \in \mathbb{K}[X]. \quad (2.1)$$

The last equality in the above formula is a result of the following proposition from [6].

Proposition 2.25 *If $f_{n,q}(X)$ is a monic separable polynomial in $\mathbb{K}[X]$, whose roots are the elements of V , then*

$$f_{n,q}(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-1} a_i X^{q^i}.$$

Proof: We have $f_{n,q}(X) := \prod_{v \in V} (X - v)$. Choose a basis e_1, e_2, \dots, e_n of V and define

$$\Delta_n(X) := \det \begin{pmatrix} e_1 & \cdots & e_n & X \\ e_1^q & \cdots & e_n^q & X^q \\ \vdots & \ddots & \vdots & \vdots \\ e_1^{q^n} & \cdots & e_n^{q^n} & X^{q^n} \end{pmatrix}.$$

Then, using column operations, we can see that each vector $v \in V$ is a root of $\Delta_n(X)$. Since $\Delta_n(X)$ is a polynomial of degree q^n , we have identified all of its roots. The coefficient of X^{q^n} is $\Delta_{n-1}(e_n)$ and as $f_{n,q}(X)$ is monic we have

$$\Delta_n(X) = \Delta_{n-1}(e_n) f_{n,q}(X).$$

It remains to verify that the constant $\Delta_{n-1}(e_n)$ is non-zero. We prove this by induction. For $n = 1$, we have $\Delta_0(e_1) = e_1 \neq 0$. Now, using the vector space V_{n-1} spanned by e_1, e_2, \dots, e_{n-1} , we get

$$\Delta_{n-1}(X) = \Delta_{n-2}(e_{n-1}) f_{n-1}(X) \neq 0$$

since $\Delta_{n-2}(e_{n-1}) \neq 0$ by the inductive hypothesis. As e_n does not belong to V_{n-1} , e_n is not a root of $\Delta_{n-1}(X)$ and therefore $\Delta_{n-1}(e_n) \neq 0$. \square

Let x_1, x_2, \dots, x_n be a basis of V^* .

Lemma 2.26 *Let U the subspace of V^* spanned by the vectors x_1, x_2, \dots, x_{n-1} . Then*

$$F_{n,q}(X) = F_{n-1,q}(X)^q - F_{n-1,q}(x_n)^{q-1} F_{n-1,q}(X)$$

where $F_{n-1,q}(X) = \prod_{u \in U} (X - u)$.

Proof: First, we note that the polynomial $F_{n,q}(X)$ is \mathbb{F}_q -linear. Hence

$$\begin{aligned} F_{n,q}(X) &= \prod_{f \in V^*} (X - f) = \prod_{a \in \mathbb{F}_q} \prod_{g \in U} (X - ax_n - g) \\ &= \prod_{a \in \mathbb{F}_q} F_{n-1,q}(X - ax_n) = \prod_{a \in \mathbb{F}_q} (F_{n-1,q}(X) - aF_{n-1,q}(x_n)) \\ &= F_{n-1,q}(X)^q - F_{n-1,q}(x_n)^{q-1} F_{n-1,q}(X). \end{aligned}$$

This finishes the proof. \square

The following example will be used frequently in Chapter 3.

Example 2.27 Let $U(n, q)$ be the group of lower triangular matrices with ones along the diagonal and x_1, \dots, x_n a basis for the dual vector space V^* . Then x_1 is invariant and the orbit of each x_i , with $i > 1$, consists of all elements $x_i + w$ where w belongs to the subspace V_{i-1} spanned by x_1, \dots, x_{i-1} .

The orbit product of each x_i is

$$N(x_i) = \prod_{w \in V_{i-1}} (x_i + w) = F_{i-1,q}(x_i),$$

where $F_{i-1,q}(X)$ is the polynomial (2.1). For example, applying Lemma 2.26 we would get $N(x_1) = x_1$, $N(x_2) = x_2^q - x_1^{q-1}x_2$, $N(x_3) = (x_3^q - x_1^{q-1}x_3)^q - N(x_2)^{q-1}(x_3^q - x_1^{q-1}x_3)$ and so on.

It can be easily proven that the polynomials $N(x_i)$ are homogeneous of degree q^{i-1} and the product of their degrees is equal to the order of $U(n, q)$. Applying Theorem 2.5 we conclude that

$$\mathbb{F}_q[V]^{U(n,q)} = \mathbb{F}_q[N(x_1), N(x_2), \dots, N(x_n)],$$

which is a polynomial ring.

Lemma 2.28 Let G_1 and G_2 be subgroups of $U(n, q^2)$ acting on $\mathbb{F}_{q^2}[V]$. Assume that for a fixed $2 \leq i \leq n$ and $l \leq i - 1$, the orbit of x_i under the action of:

- G_1 is $\{x_i + \sum_{j=1}^l a_j x_j : a_1, \dots, a_{l-1} \in \mathbb{F}_{q^2} \wedge a_l \in \mathbb{F}_q\}$;

- G_2 is $\{x_i + \sum_{j=1}^l a_j x_j : a_1, \dots, a_{l-1} \in \mathbb{F}_{q^2} \wedge a_l + \bar{a}_l = 0\}$.

Then the orbit product of x_i is given by:

1. $N(x_i) = F_{l-1,q^2}(x_i)^q - F_{l-1,q^2}(x_l)^{q-1} F_{l-1,q^2}(x_i)$ if $a_l \in \mathbb{F}_q$,
2. $N(x_i) = F_{l-1,q^2}(x_i)^q + F_{l-1,q^2}(x_l)^{q-1} F_{l-1,q^2}(x_i)$ if $a_l + \bar{a}_l = 0$.

Moreover, both are homogeneous polynomials of degree q^{2l-1} .

Proof: Let V be the vector space over \mathbb{F}_{q^2} spanned by x_1, \dots, x_{l-1} . Then

$$F_{l-1,q^2}(X) = \prod_{a_1, \dots, a_{l-1} \in \mathbb{F}_{q^2}} (X + a_1 x_1 + \dots + a_{l-1} x_{l-1})$$

and it is homogeneous of degree q^{2l-2} . Since $F_{l-1,q^2}(X)$ is \mathbb{F}_{q^2} -linear, replacing X by $x_i + a_l x_l$ gives

$$F_{l-1,q^2}(x_i) + a_l F_{l-1,q^2}(x_l) = \prod_{a_1, \dots, a_{l-1} \in \mathbb{F}_{q^2}} (x_i + a_l x_l + a_1 x_1 + \dots + a_{l-1} x_{l-1}).$$

Therefore, we get

$$N(x_i) = \prod_{a_l \in \mathbb{F}_q} (F_{l-1,q^2}(x_i) + a_l F_{l-1,q^2}(x_l)) = F_{l-1,q^2}(x_i)^q - F_{l-1,q^2}(x_l)^{q-1} F_{l-1,q^2}(x_i)$$

for the orbit product of x_i under the action of G_1 .

Now, for the action of G_2 the orbit product of x_i is given by

$$N(x_i) = \prod_{a_l + \bar{a}_l = 0} (F_{l-1,q^2}(x_i) + a_l F_{l-1,q^2}(x_l)).$$

Note that $a_l + \bar{a}_l = 0$ is equivalent to say that $a_l \in \ker \text{Tr}$. According to Lemma 1.13, $\ker \text{Tr}$ is a one dimensional vector space over \mathbb{F}_q . So if $c \notin \mathbb{F}_q$, then $c - \bar{c}$ is a basis for $\ker \text{Tr}$ and

$$N(x_i) = \prod_{a \in \mathbb{F}_q} (F_{l-1,q^2}(x_i) + a(c - \bar{c}) F_{l-1,q^2}(x_l)) = F_{l-1,q^2}(x_i)^q - ((c - \bar{c}) F_{l-1,q^2}(x_l))^{q-1} F_{l-1,q^2}(x_i).$$

Since $(c - \bar{c})^{q-1} = -1$, the statement in 2 is proved. \square

2.4.2 Steenrod Operations

The Steenrod operations are a helpful tool in invariant theory to construct new invariants from old ones. They will play an important role in Chapters 3 and 4.

Suppose that $\mathbb{F} = \mathbb{F}_q$ is a finite field. We take an additional indeterminate T and we define a map

$$\mathcal{P}(T) : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V][T]$$

by the rules:

- (i) $\mathcal{P}(T)(x) = x + x^q T$ for all $x \in V^*$;
- (ii) $\mathcal{P}(T)(fg) = \mathcal{P}(T)(f)\mathcal{P}(T)(g)$ for all $f, g \in \mathbb{F}_q[V]$;
- (iii) $\mathcal{P}(T)(1) = 1$.

It is not hard to check that $\mathcal{P}(T)$ is in fact a homomorphism of \mathbb{F} -algebras and that it commutes with the action of $GL(V)$ on $\mathbb{F}_q[V]$.

If for $f \in \mathbb{F}_q[V]$ we write

$$\mathcal{P}(T)(f) = \sum_{i \geq 0} \mathcal{P}^i(T)(f) T^i$$

then $\mathcal{P}^i(T)(f)$ is called the i -th **Steenrod operation** on f . Hence, if f is an invariant then $\mathcal{P}^i(T)(f)$ is again an invariant.

It is easily checked that for an homogeneous polynomial f we have:

- $\mathcal{P}^i(T)(f) = \begin{cases} f^q & \text{if } i = \deg f \\ 0 & \text{if } i > \deg f \end{cases}$
- $\mathcal{P}^k(T)(fg) = \sum_{i+j=k} \mathcal{P}^i(T)(f)\mathcal{P}^j(T)(g)$.
- If $\mathcal{P}^i(T)(f) \neq 0$ then $\deg(\mathcal{P}^i(T)(f)) = \deg(f) + i(q-1)$.

2.5 *SAGBI* Bases

In this section we introduce the concept of *SAGBI* bases, which was first considered by Robbiano & Sweedler [24] and by Kapur & Madlener [15], separately. The acronym *SAGBI* stands for “Subalgebra Analogs to Gröbner Bases for Ideals”. *SAGBI* bases allow us to answer the subalgebra membership question.

In Chapter 4, we will consider finitely generated subalgebras for which we can prove that their generators are in fact *SAGBI* bases. To this end, we need to address the following problem: given a finite set B of generators for an algebra $A \subseteq \mathbb{F}[x_1, \dots, x_n]$, when is B a *SAGBI* basis for A ? We use the approach given in [26] as a way to solve this.

A **monomial** in $\mathbb{F}[x_1, \dots, x_n]$ is an element of the form $x_1^{a_1} \cdots x_n^{a_n}$ with a_i non-negative integers. Let \mathcal{M} be the set of all monomials. A **term** is an element of the form cm where $c \in \mathbb{F} \setminus \{0\}$ and $m \in \mathcal{M}$.

Definition 2.29 A *monomial order* is a total order $>$ on \mathcal{M} satisfying the following conditions:

- (i) $m > 1$ for all $m \in \mathcal{M} \setminus \{1\}$,
- (ii) $m_1 > m_2$ implies $mm_1 > mm_2$ for all $m, m_1, m_2 \in \mathcal{M}$.

Fix a monomial order $<$ on \mathcal{M} . Then a non-zero polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ can be written uniquely as $f = cm + g$ such that $m \in \mathcal{M}$, $c \in \mathbb{F} \setminus \{0\}$ and every term of g is smaller than m . We write

$$LT(f) = cm, \quad LM(f) = m, \quad \text{and} \quad LC(f) = c$$

for the **leading term**, **leading monomial** and **leading coefficient** of f , respectively. If f is zero, then all three values are defined to be zero.

Example 2.30 Let $m_1 = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $m_2 = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ be two distinct monomial. Then in the **lexicographic order** $m_1 <_{lex} m_2$ if $a_i < b_i$ for the smallest i such that $a_i \neq b_i$. As an example, $LM(x_1 + x_2 x_4 + x_3^2) = x_1$.

Example 2.31 Let $m_1 = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $m_2 = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ be two distinct monomials. Then in the **graded reverse lexicographic order** $m_1 <_{grevlex} m_2$ 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 $a_i \neq b_i$. Again as an example, $LM(x_1 + x_2 x_4 + x_3^2) = x_3^2$.

We would like to note that the definition in the previous example is not the one usually found in the literature. We decide to do it in this way because we want the monomials that have x_1 to be smaller than those who do not. This is will be crucial to obtain the results in Chapter 4.

Suppose that A is a subalgebra of $\mathbb{F}[x_1, \dots, x_n]$ and that we have chosen some monomial ordering, $<$, on the monomials of $\mathbb{F}[x_1, \dots, x_n]$. We write $LT(A)$ for the algebra generated by all leading monomials of non-zero elements of A .

Definition 2.32 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 $C := \{f_1, f_2, \dots, f_m\}$ be a finite set of polynomials in $\mathbb{F}[x_1, x_2, \dots, x_n]$ and A the \mathbb{F} -algebra generated by them.

Let $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$. The **subduction** of f over C is performed as follows:

1. Set $h := f$.
2. If h is a constant in \mathbb{F} then stop, otherwise go to step 3.
3. Check if there exist $c \in \mathbb{F}$ and exponents $u_1, u_2, \dots, u_m \in \mathbb{N}$ such that $LT(h) := c \prod_{j=1}^m LM(f_j)^{u_j}$.
4. If step 3. fails then stop, otherwise go to step 5.

5. Replace h by $h - c \prod_{j=1}^m f_j^{u_j}$ and go to step 2.

Note that each time we get to step 5., 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 it is always possible to perform step 3. in the subduction of f over C and when we reach the end of the procedure we will be able to write f as a polynomial expression in f_1, \dots, f_m . Therefore, if $f \notin A$ then at some stage in the subduction process, step 3. will fail. Hence when C is a *SAGBI* basis the subduction process can be used as an algebra membership test.

We consider the sequence (f_1, \dots, f_m) with $f_i \in C$ for all i .

Definition 2.33 *A tête-a-tête over (f_1, \dots, f_m) 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

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

is either a constant or has a smaller leading monomial.

Theorem 2.34 *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 [24], Theorem 2.8. \square

We present here another criterion to check whether C is a *SAGBI* basis for A or not.

For each f_i , with $i = 1, \dots, m$, we associate its leading monomial with a vector $\mathbf{a}_i \in \mathbb{N}^n$ by

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

Define the algebra homomorphism

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

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 $\pi(\mathbf{u}) = \pi(u_1, u_2, \dots, u_m) = u_1 \mathbf{a}_1 + u_2 \mathbf{a}_2 + \dots + u_m \mathbf{a}_m$.

Theorem 2.35 *Assume that g_1, g_2, \dots, 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 $g_i(f_1, \dots, f_m)$ terminates at a constant for all $i \in \{1, \dots, s\}$.*

Proof: See Corollary 11.5 in [26]. \square

Corollary 2.36 *Let f_1, \dots, f_n be polynomials in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$ such that $LM(f_i) = x_i^{d_i}$ with d_i a non-negative integer. Then $\{f_1, \dots, f_n\}$ 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 2.35 finishes the proof. \square

In order to apply Theorem 2.35 we must be able to compute the generators for the kernel of ϕ . We shall write $\mathbf{T}^{\mathbf{u}}$, $\mathbf{u} \in \mathbb{N}^m$, for the monomial $\prod_{j=1}^m t_j^{u_j}$.

Lemma 2.37 *The kernel of the homomorphism ϕ is spanned as a \mathbb{F} -vector space by the set of binomials*

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

Proof: See Lemma 4.1 in [26]. \square

Remark 2.38 *The previous Lemma shows that kernel of ϕ is spanned by the binomials $\mathbf{T}^{\mathbf{u}} - \mathbf{T}^{\mathbf{v}}$ where (\mathbf{u}, \mathbf{v}) is a tête-a-tête.*

For any tuple of integers $\mathbf{u} = (u_1, \dots, u_m) \in \mathbb{Z}^m$, we let $\mathbf{u}^+ = (u_1^+, \dots, u_m^+)$ and $\mathbf{u}^- = (u_1^-, \dots, u_m^-)$ 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 2.39 *The kernel of ϕ is spanned by the binomials*

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

Define a $n \times m$ matrix B whose columns are the vectors \mathbf{a}_i corresponding to the lead monomials of the polynomials f_i . It is not hard to see that $\mathbf{u} \in \mathbb{Z}^m$ belongs to the $\ker \pi$ 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 consisting of all the solutions for $B\mathbf{u} = 0$. 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 2.40 *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 $\mathbf{T}^{\mathbf{w}^+} - \mathbf{T}^{\mathbf{w}^-}$.*

Proof: According to Corollary 2.39, we get the result if we can show that for any element $\mathbf{u} \in \ker \pi$ the binomial $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-}$ is an element in the ideal generated by $\mathbf{T}^{\mathbf{w}^+} - \mathbf{T}^{\mathbf{w}^-}$.

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

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

and therefore it belongs to ideal generated by $\mathbf{T}^{\mathbf{w}^+} - \mathbf{T}^{\mathbf{w}^-}$. This finishes the proof. \square

Finally, we consider the case when the dimension of W is 2. We will need the following hypothesis:

Hypothesis A: We assume that $\{\mathbf{w}_1, \mathbf{w}_2\} \subset \mathbb{Z}^m$ is a basis for W satisfying the following properties:

1. Any linear combination $\alpha_1 \mathbf{w}_1 + \alpha_2 \mathbf{w}_2$ belongs to \mathbb{Z}^m if and only if $\alpha_1, \alpha_2 \in \mathbb{Z}$.
2. For any vector $\mathbf{u} = \alpha_1 \mathbf{w}_1 + \alpha_2 \mathbf{w}_2 \in \mathbb{Z}^m$, one of the following holds:
 - (a) The vectors $\mathbf{u}^+ - (\alpha_1 \mathbf{w}_1)^+$ and $\mathbf{u}^- - (\alpha_2 \mathbf{w}_2)^-$ have non-negative entries.
 - (b) The vectors $\mathbf{u}^+ - (\alpha_2 \mathbf{w}_2)^+$ and $\mathbf{u}^- - (\alpha_1 \mathbf{w}_1)^-$ have non-negative entries.

Let $\{\mathbf{w}_1, \mathbf{w}_2\}$ be a basis of W for which **Hypothesis A** holds. Then, we define the set

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

Obviously, we have $\mathcal{F} \subseteq \ker \pi$.

Proposition 2.41 *Under the above assumptions, the kernel of ϕ is generated as an ideal by the binomials in the set \mathcal{F} .*

Proof: Just as in Lemma 2.40, it is enough to show that for any element $\mathbf{u} \in \ker \pi$ the binomial $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-}$ is an element in the ideal $\langle \mathcal{F} \rangle$ generated by \mathcal{F} . Then, the result will follow from Corollary 2.39.

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 it was done in the proof of Lemma 2.40 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 $\langle \mathcal{F} \rangle$.

Now, we shall prove that $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-} \in \langle \mathcal{F} \rangle$. 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 2(a) in **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 2(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 $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-} \in \langle \mathcal{F} \rangle$ and the proof is complete. \square

We illustrate how we can use all the above results with the following example.

Example 2.42 Let A be the subalgebra of $\mathbb{F}_q[x_1, x_2]$ generated by the polynomials $f_1 = x_1^q$, $f_2 = x_2^q$, $f_3 = x_2x_1$ and $f_4 = x_2^qx_1 + x_2x_1^q$. Also, consider the graded reverse lexicographic order with $x_2 > x_1$. We will show that $C = \{f_1, f_2, f_3, f_4\}$ is a SAGBI basis for A .

Here the \mathbb{F}_q -algebra homomorphism $\phi : \mathbb{F}_q[t_1, t_2, t_3, t_4] \longrightarrow \mathbb{F}_q[x_1, x_2]$ is defined by

$$t_1 \mapsto x_1^q, \quad t_2 \mapsto x_2^q, \quad t_3 \mapsto x_2x_1, \quad t_4 \mapsto x_2^qx_1.$$

Then the matrix B is

$$\begin{pmatrix} q & 0 & 1 & 1 \\ 0 & q & 1 & q \end{pmatrix}$$

and it has rank 2. Therefore the solution set for $B\mathbf{u} = 0$ is a 2-dimensional real vector space W . It is not hard to check that the vectors

$$\mathbf{w}_1 := (0, 0, q, 0) - (1, 1, 0, 0) = (-1, -1, q, 0)$$

$$\mathbf{w}_2 := (0, 0, 0, q) - (1, q, 0, 0) = (-1, -q, 0, q)$$

form a basis for W .

First, we check that **Hypothesis A** 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 $-\alpha_1 - \alpha_2$, $-\alpha_1 - \alpha_2q$, α_1q and α_2q are integers. Thus α_1 and α_2 must be integers.

Now, let $\mathbf{u} = \alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2 = (-\alpha_1 - \alpha_2, -\alpha_1 - \alpha_2q, \alpha_1q, \alpha_2q) \in \mathbb{Z}^4$. We have to consider four different cases:

1. For $\alpha_1 \geq 0$ and $\alpha_2 \geq 0$ we get

$$\begin{aligned}\mathbf{u}^+ &= (0, 0, \alpha_1 q, \alpha_2 q), & \mathbf{u}^- &= (\alpha_1 + \alpha_2, \alpha_1 + \alpha_2 q, 0, 0) \\ (\alpha_1 \mathbf{w}_1)^+ &= (0, 0, \alpha_1 q, 0), & \text{and } (\alpha_2 \mathbf{w}_2)^- &= (\alpha_2, \alpha_2 q, 0, 0).\end{aligned}$$

Therefore 2.(a) in **Hypothesis A** is satisfied.

2. For $\alpha_1 \leq 0$ and $\alpha_2 \leq 0$ we get

$$\begin{aligned}\mathbf{u}^+ &= (-\alpha_1 - \alpha_2, -\alpha_1 - \alpha_2 q, 0, 0), & \mathbf{u}^- &= (0, 0, -\alpha_1 q, -\alpha_2 q) \\ (\alpha_1 \mathbf{w}_1)^+ &= (-\alpha_1, -\alpha_1, 0, 0), & \text{and } (\alpha_2 \mathbf{w}_2)^- &= (0, 0, 0, -\alpha_2 q).\end{aligned}$$

Again, we can easily see that 2.(a) in **Hypothesis A** is satisfied.

3. If $\alpha_1 < 0$ and $\alpha_2 > 0$, then

$$(\alpha_1 \mathbf{w}_1)^- = (0, 0, -\alpha_1 q, 0) \quad \text{and} \quad (\alpha_2 \mathbf{w}_2)^+ = (0, 0, 0, \alpha_2 q).$$

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 $u_4^+ = \alpha_2 q$ and $u_3^- = -\alpha_1 q$, it follows that 2.(b) in **Hypothesis A** is satisfied.

4. Finally, if $\alpha_1 > 0$ and $\alpha_2 < 0$, then

$$(\alpha_1 \mathbf{w}_1)^+ = (0, 0, \alpha_1 q, 0) \quad \text{and} \quad (\alpha_2 \mathbf{w}_2)^- = (0, 0, 0, -\alpha_2 q).$$

Now, since $u_3^+ = \alpha_1 q$ and $u_4^- = -\alpha_2 q$, it follows that 2.(a) in **Hypothesis A** is satisfied.

Hence, by Proposition 2.41, $g_1(t_1, t_2, t_3, t_4) = t_3^q - t_1 t_2$ 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. Since

$$f_3^q - f_1 f_2 = 0 \quad \text{and} \quad f_4^q - f_1 f_2^q - f_1^q f_2 = 0$$

we conclude that there exist a subduction for $g_1(f_1, f_2, f_3, f_4)$ and $g_2(f_1, f_2, f_3, f_4)$ over C that terminates at a constant. Therefore, it follows from Theorem 2.35 that C is a SAGBI basis for A .

Chapter 3

Invariant Fields for Sylow p -subgroups of Finite Classical Groups

In this chapter we construct the generators for the invariant fields for all the Sylow p -subgroups introduced in Chapter 1. We apply the algorithm described in Section 2.3. All the results will follow from Theorem 2.23 except for the Sylow p -subgroups of the orthogonal groups $O^+(2m, q)$ and $O^-(2m + 2, q)$ in characteristic 2. For these we will also need to use Remark 2.21.

Since the calculations we need to construct the generators for the invariant field of each group are similar, we start by establishing some general lemmas and propositions. This is done in the first section. Here we introduce some families of polynomials and we determine the action of the Steenrod operations on them. Also, we consider two families of subgroups of $U(n, \mathbb{F})$ whose invariants will be used to determine lower bounds for the minimal degree in x_j of an invariant polynomial in $R[j] = \mathbb{F}[x_1, \dots, x_j]$. Then applying the results established in this section we finish the chapter by computing the generators for each invariant field.

3.1 Preliminary Results

Let \mathbb{F} be either the finite field \mathbb{F}_q or \mathbb{F}_{q^2} and V be a n -dimensional vector space over \mathbb{F} . We denote by r the number of elements of \mathbb{F} . We consider the symmetric algebra $A := \mathbb{F}[V] = \mathbb{F}[x_1, \dots, x_n]$. Recall that $U(n, \mathbb{F})$ is the group of $n \times n$ lower triangular matrices with entries in \mathbb{F} and with ones along the diagonal.

In Example 2.27 of Subsection 2.4.1 we have seen that

$$\mathbb{F}[V]^{U(n, \mathbb{F})} = \mathbb{F}[N(x_1), N(x_2), \dots, N(x_n)]$$

where $N(x_i)$ is the orbit product of x_i . Moreover, $N(x_i) = F_{i-1, r}(x_i)$ where $F_{i-1, r}(X)$ is the polynomial (2.1), which according to Lemma 2.26 can be computed recursively as follows:

$$F_{n, r}(X) = F_{n-1, r}(X)^r - F_{n-1, r}(x_n)^{r-1} F_{n-1, r}(X) \text{ for } n \geq 1 \text{ and } F_{0, r}(X) = X.$$

We define a sequence of endomorphisms ψ_l of \mathbb{F} -algebras from A to itself by

$$\psi_l : A \longrightarrow A, \quad x_i \mapsto F_{l, r}(x_i).$$

Note that ψ_0 is the identity map on A , $\psi_1(x_1) = 0$ 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 $U(n, \mathbb{F})$.

Proposition 3.1 *For every endomorphism ψ_l the following hold:*

1. $\psi_l(x_k) = 0$ for all $1 \leq k \leq l$;
2. $\psi_l(x_{l+1})$ is an invariant polynomial under the action of $U(n, \mathbb{F})$;
3. $\psi_l(f) = (\psi_{l-1}(f))^r - \psi_{l-1}(x_l)^{r-1} \psi_{l-1}(f)$ for every homogeneous polynomial f in degree 1, i.e, \mathbb{F} -linear combinations of the x_i 's;
4. for every $g \in U(n, \mathbb{F})$ we have $g \circ \psi_l = \psi_l \circ g$.

Proof: We prove 1. by induction on l . For $l = 1$ we have seen that $\psi_1(x_1) = 0$. Now we assume that the statement is true for l and let $k \leq l + 1$. Then

$$\psi_{l+1}(x_k) = \psi_l(x_k)^r - \psi_l(x_{l+1})^{r-1}\psi_l(x_k),$$

which is zero for $k \leq l$ by the induction hypothesis. For $k = l + 1$ we get $\psi_{l+1}(x_{l+1}) = 0$ immediately.

By definition $\psi_l(x_{l+1}) = F_{l,r}(x_{l+1})$ and we have seen in Example 2.27 that $F_l(x_{l+1})$ is the orbit product of x_{l+1} under the action of $U(n, \mathbb{F})$. Hence 2. is proved.

To prove 3., note that the endomorphisms ψ_l as well as multiplication by the fixed element $\psi_{l-1}(x_l)^{r-1}$ are \mathbb{F} -linear operators. Since the formula is true for each x_i by definition, the result follows.

Finally, we show that 4. holds. It suffices to show that $(g \circ \psi_l)(x_i) = (\psi_l \circ g)(x_i)$ for all $i = 1, 2, \dots, n$. Again, we use induction on l . For $l = 0$ the result follows immediately since ψ_0 is the identity map. We assume that the result holds for l . Then

$$\begin{aligned} (g \circ \psi_{l+1})(x_i) &= g(\psi_{l+1}(x_i)) = g(\psi_l(x_i)^r - \psi_l(x_{l+1})^{r-1}\psi_l(x_i)) \\ &= (g(\psi_l(x_i)))^r - (g(\psi_l(x_{l+1})))^{r-1}(g(\psi_l(x_i))) \\ &= \psi_l(g(x_i))^r - \psi_l(g(x_{l+1}))^{r-1}\psi_l(g(x_i)) \end{aligned}$$

where we have used the induction hypothesis. It follows from 2 that $\psi_l(x_{l+1})$ is invariant and therefore $\psi_l(g(x_{l+1})) = \psi_l(x_{l+1})$. Hence

$$\begin{aligned} (g \circ \psi_{l+1})(x_i) &= \psi_l(g(x_i))^r - \psi_l(x_{l+1})^{r-1}\psi_l(g(x_i)) \\ &= (\psi_{l+1} \circ g)(x_i) \end{aligned}$$

and this finishes the proof. \square

We consider the following families of polynomials in $\mathbb{F}[x_1, \dots, x_n]$. We use two parameters: $j \in \{-1, 1\}$ and $\lambda \in \{0, 1\}$. Fix an element $c \in \mathbb{F}$ and let $m = \frac{n}{2}$ or $m = \frac{n-1}{2}$ if n is even or odd, respectively. Now define

- $\Omega_{0,1} = \sum_{i=1}^m x_{n-i+1}x_i$ and $\Omega_{0,-1} = 0$;
- $\Omega_{s,j} = \sum_{i=1}^m (x_{n-i+1}^{r^s}x_i + jx_{n-i+1}x_i^{r^s})$ for $s \geq 1$;
- $\Gamma_{0,\lambda} = \Omega_{0,1} + x_{m+1}^2 + c\lambda x_{m+2}^2$;
- $\Gamma_{s,\lambda} = \Omega_{s,1} + 2(x_{m+1}^{r^s+1} + c\lambda x_{m+2}^{r^s+1})$ for $s \geq 1$ and here 2 is the modulo p reduction of the integer 2 with p being the characteristic of \mathbb{F} ;
- $\Lambda_{s,\lambda} = \sum_{i=1}^m (x_{n-i+1}^{q^{2s-1}}x_i + x_{n-i+1}x_i^{q^{2s-1}}) + \lambda x_{m+1}^{q^{2s-1}+1}$ for $s \geq 1$ and $\mathbb{F} = \mathbb{F}_{q^2}$.

We will apply the Steenrod operations to these polynomials. See Subsection 2.4.2 for its definition. Here we take $T = -1$ and we denote $\mathcal{P}(-1)$ by \mathcal{P}^\bullet . Hence $\mathcal{P}^\bullet : A \longrightarrow A$ is the \mathbb{F} -algebra homomorphism given by $\mathcal{P}^\bullet(x_i) = x_i - x_i^r$. Also,

$$\mathcal{P}^\bullet(f) = \mathcal{P}^0(f) - \mathcal{P}^1(f) + \mathcal{P}^2(f) - \mathcal{P}^3(f) + \dots$$

where $\mathcal{P}^i(f)$ is the i -th Steenrod operation on f .

Proposition 3.2 *Let $\Omega_{s,j}$, $\Gamma_{s,\lambda}$ and $\Lambda_{s,\lambda}$ be the polynomials defined above. Then:*

1. $\mathcal{P}^\bullet(\Omega_{0,1}) = \Omega_{0,1}^r - \Omega_{1,1} + \Omega_{0,1}$;
2. $\mathcal{P}^\bullet(\Omega_{1,1}) = \Omega_{1,1}^r - \Omega_{2,1} - 2\Omega_{0,1}^r + \Omega_{1,1}$;
3. $\mathcal{P}^\bullet(\Omega_{s,j}) = \Omega_{s,j}^r - \Omega_{s+1,j} - \Omega_{s-1,j}^r + \Omega_{s,j}$ for $s > 0$ if $j = -1$ and $s > 1$ if $j = 1$;
4. $\mathcal{P}^\bullet(\Gamma_{0,\lambda}) = \Gamma_{0,\lambda}^r - \Gamma_{1,\lambda} + \Gamma_{0,\lambda}$;
5. $\mathcal{P}^\bullet(\Gamma_{1,\lambda}) = \Gamma_{1,\lambda}^r - \Gamma_{2,\lambda} - 2\Gamma_{0,\lambda}^r + \Gamma_{1,\lambda}$;
6. $\mathcal{P}^\bullet(\Gamma_{s,\lambda}) = \Gamma_{s,\lambda}^r - \Gamma_{s+1,\lambda} - \Gamma_{s-1,\lambda}^r + \Gamma_{s,\lambda}$ for $s > 1$;
7. $\mathcal{P}^\bullet(\Lambda_{1,\lambda}) = \Lambda_{1,\lambda}^{q^2} - \Lambda_{2,\lambda} - \Lambda_{1,\lambda}^q + \Lambda_{1,\lambda}$;
8. $\mathcal{P}^\bullet(\Lambda_{s,\lambda}) = \Lambda_{s,\lambda}^{q^2} - \Lambda_{s+1,\lambda} - \Lambda_{s-1,\lambda}^{q^2} + \Lambda_{s,\lambda}$ for $s \geq 2$.

Proof: Applying \mathcal{P}^\bullet to $\Omega_{0,1}$ we obtain

$$\begin{aligned}\mathcal{P}^\bullet(\Omega_{0,1}) &= \sum_{i=1}^m \mathcal{P}^\bullet(x_{n-i+1}) \mathcal{P}^\bullet(x_i) = \sum_{i=1}^m (x_{n-i+1} - x_{n-i+1}^r)(x_i - x_i^r) \\ &= \Omega_{0,1} - \Omega_{1,1} + \Omega_{0,1}^r\end{aligned}$$

and 1 is proved. Now

$$\begin{aligned}\mathcal{P}^\bullet(\Omega_{s,j}) &= \sum_{i=1}^m (\mathcal{P}^\bullet(x_{n-i+1})^{r^s} \mathcal{P}^\bullet(x_i) + j \mathcal{P}^\bullet(x_{n-i+1}) \mathcal{P}^\bullet(x_i)^{r^s}) \\ &= \sum_{i=1}^m ((x_{n-i+1}^{r^s} - x_{n-i+1}^{r^{s+1}})(x_i - x_i^r) + j(x_{n-i+1} - x_{n-i+1}^r)(x_i^{r^s} - x_i^{r^{s+1}}))\end{aligned}$$

and from this 2 and 3 follow.

Before proving 4, 5 and 6 note that by taking

$$f_{s,\lambda} := x_{m+1}^{r^s+1} + c\lambda x_{m+2}^{r^s+1}$$

we can write

$$\Gamma_{0,\lambda} = \Omega_{0,1} + f_{0,\lambda}, \quad \Gamma_{s,\lambda} = \Omega_{s,1} + 2f_{s,\lambda}.$$

Thus,

$$\mathcal{P}^\bullet(\Gamma_{0,\lambda}) = \mathcal{P}^\bullet(\Omega_{0,1}) + \mathcal{P}^\bullet(f_{0,\lambda}), \quad \mathcal{P}^\bullet(\Gamma_{s,\lambda}) = \mathcal{P}^\bullet(\Omega_{s,1}) + 2\mathcal{P}^\bullet(f_{s,\lambda})$$

and therefore we just need to determine how \mathcal{P}^\bullet acts on the polynomials $f_{s,\lambda}$. Following the same reasoning as in the beginning of the proof, we can show that

$$\begin{aligned}\mathcal{P}^\bullet(f_{0,\lambda}) &= f_{0,\lambda}^r - 2f_{1,\lambda} + f_{0,\lambda}; \\ \mathcal{P}^\bullet(f_{s,\lambda}) &= f_{s,\lambda}^r - f_{s+1,\lambda} - f_{s-1,\lambda}^r + f_{s,\lambda} \quad \text{for } s > 0.\end{aligned}$$

Combining this with the results in 1, 2 and 3 we get 4, 5 and 6.

We only prove 7. Since in this case $\mathbb{F} = \mathbb{F}_{q^2}$, we have $r = q^2$ and so

$$\begin{aligned}
\mathcal{P}^\bullet(\Lambda_{1,\lambda}) &= \sum_{i=1}^m (\mathcal{P}^\bullet(x_{n-i+1})^q \mathcal{P}^\bullet(x_i) + \mathcal{P}^\bullet(x_{n-i+1}) \mathcal{P}^\bullet(x_i)^q) + \lambda \mathcal{P}^\bullet(x_{m+1}^{q+1}) \\
&= \sum_{i=1}^m ((x_{n-i+1}^q - x_{n-i+1}^{q^3})(x_i - x_i^{q^2}) + (x_{n-i+1} - x_{n-i+1}^{q^2})(x_i^q - x_i^{q^3})) \\
&\quad + \lambda(x_{m+1}^q - x_{m+1}^{q^3})(x_{m+1} - x_{m+1}^{q^2}) \\
&= \Lambda_{1,\lambda}^{q^2} - \Lambda_{2,\lambda} - \Lambda_{1,\lambda}^q + \Lambda_{1,\lambda}.
\end{aligned}$$

A similar calculation proves 8. \square

Corollary 3.3 *The Steenrod operations on the polynomials $\Omega_{s,j}$, $\Gamma_{s,\lambda}$ and $\Lambda_{s,\lambda}$ are given by:*

1. $\mathcal{P}^1(\Omega_{0,1}) = \Omega_{1,1}$, $\mathcal{P}^1(\Gamma_{0,\lambda}) = \Gamma_{1,\lambda}$ and $\mathcal{P}^1(\Lambda_{1,\lambda}) = \Lambda_{1,\lambda}^q$;
2. $\mathcal{P}^1(\Omega_{1,1}) = 2\Omega_{0,1}^r$, $\mathcal{P}^1(\Omega_{s,j}) = \Omega_{s-1,j}^r$ for $s \geq 2$, $\mathcal{P}^1(\Gamma_{s,\lambda}) = \Gamma_{s-1,\lambda}^r$ for $s \geq 1$ and $\mathcal{P}^1(\Lambda_{s,\lambda}) = \Lambda_{s,\lambda}^{q^2}$ for $s \geq 2$;
3. $\mathcal{P}^{r^s}(\Omega_{s,j}) = \Omega_{s+1,j}$, $\mathcal{P}^{r^s}(\Gamma_{s,\lambda}) = \Gamma_{s+1,\lambda}$ and $\mathcal{P}^{q^{2s-1}}(\Lambda_{s,\lambda}) = \Lambda_{s+1,\lambda}$ for $s \geq 1$;
4. $\mathcal{P}^{r^{s+1}}(\Omega_{s,j}) = \Omega_{s,j}^r$, $\mathcal{P}^{r^{s+1}}(\Gamma_{s,\lambda}) = \Gamma_{s,\lambda}^r$ for $s \geq 0$ and $\mathcal{P}^{q^{2s-1}+1}(\Lambda_{s,\lambda}) = \Lambda_{s,\lambda}^{q^2}$ for $s \geq 1$;
5. $\mathcal{P}^i(\Omega_{s,j}) = 0$, $\mathcal{P}^i(\Gamma_{s,\lambda}) = 0$ and $\mathcal{P}^i(\Lambda_{s,\lambda}) = 0$, otherwise.

Proof: We will prove the result only for the polynomials $\Omega_{s,j}$.

For an homogeneous polynomial f such that the i -th steenrod operation $\mathcal{P}^i(f) \neq 0$, we obtain $\deg(\mathcal{P}^i(f)) = \deg(f) + i(r-1)$. Thus, we just need to consider the degrees of the terms in $\mathcal{P}^\bullet(\Omega_{0,1})$ and $\mathcal{P}^\bullet(\Omega_{s,j})$. We have

$$\mathcal{P}^\bullet(\Omega_{0,1}) = \mathcal{P}^0(\Omega_{0,1}) - \mathcal{P}^1(\Omega_{0,1}) + \mathcal{P}^2(\Omega_{0,1}) - \mathcal{P}^3(\Omega_{0,1}) + \cdots = \Omega_{0,1}^r - \Omega_{1,1} + \Omega_{0,1}$$

by Proposition 3.2. The degrees of $\Omega_{0,1}$, $\Omega_{1,1}$ and $\Omega_{0,1}^r$ are 2, $r+1$ and $2r$, respectively. Comparing this with the degrees of $\mathcal{P}^i(\Omega_{0,1})$, we get $\mathcal{P}^0(\Omega_{0,1}) = \Omega_{0,1}$, $\mathcal{P}^1(\Omega_{0,1}) = \Omega_{1,1}$ and $\mathcal{P}^2(\Omega_{0,1}) = \Omega_{0,1}^r$. Again by Proposition 3.2 we get for $s > 0$,

$$\begin{aligned}\mathcal{P}^\bullet(\Omega_{1,1}) &= \mathcal{P}^0(\Omega_{1,1}) - \mathcal{P}^1(\Omega_{1,1}) + \mathcal{P}^2(\Omega_{1,1}) - \cdots = \Omega_{1,1}^r - \Omega_{2,1} - 2\Omega_{0,1}^r + \Omega_{1,1}, \\ \mathcal{P}^\bullet(\Omega_{s,j}) &= \Omega_{s,j}^r - \Omega_{s+1,j} - \Omega_{s-1,j}^r + \Omega_{s,j}.\end{aligned}$$

Hence

- $\mathcal{P}^0(\Omega_{s,j}) = \Omega_{s,j}$;
- $\deg \Omega_{s-1,j}^r = r(r^{s-1} + 1)$, $\deg \mathcal{P}^1(\Omega_{s,j}) = r^s + 1 + r - 1$ and therefore $\mathcal{P}^1(\Omega_{1,1}) = 2\Omega_{0,1}^r$ and $\mathcal{P}^1(\Omega_{s,j}) = \Omega_{s-1,j}^r$;
- $\deg \Omega_{s+1,j} = r^{s+1} + 1$, $\deg \mathcal{P}^{r^s}(\Omega_{s,j}) = r^s + 1 + r^s(r-1)$ and therefore $\mathcal{P}^{r^s}(\Omega_{s,j}) = \Omega_{s+1,j}$;
- $\deg \Omega_{s,j}^r = r(r^s + 1)$, $\deg \mathcal{P}^{r^s+1}(\Omega_{s,j}) = r^s + 1 + (r^s + 1)(r-1)$ and therefore $\mathcal{P}^{r^s+1}(\Omega_{s,j}) = \Omega_{s,j}^r$;

Similar arguments prove the remaining results in the corollary. \square

The next proposition shows how the \mathbb{F} -algebra homomorphism ψ_l acts on the polynomials $\Omega_{s,j}$, $\Gamma_{s,\lambda}$ and $\Lambda_{s,\lambda}$.

Proposition 3.4 *For every $l \geq 1$, the following is true:*

1. $\psi_l(\Omega_{0,1}) = \psi_{l-1}(\Omega_{0,1})^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(\Omega_{1,1}) + \psi_{l-1}(x_l)^{2(r-1)}\psi_{l-1}(\Omega_{0,1})$;
2. $\psi_l(\Omega_{1,1}) = \psi_{l-1}(\Omega_{1,1})^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(\Omega_{2,1}) - 2\psi_{l-1}(x_l)^{r(r-1)}\psi_{l-1}(\Omega_{0,1})^r + \psi_{l-1}(x_l)^{(r+1)(r-1)}\psi_{l-1}(\Omega_{1,1})$;
3. $\psi_l(\Omega_{s,j}) = \psi_{l-1}(\Omega_{s,j})^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(\Omega_{s+1,j}) - \psi_{l-1}(x_l)^{r^s(r-1)}\psi_{l-1}(\Omega_{s-1,j})^r + \psi_{l-1}(x_l)^{(r^s+1)(r-1)}\psi_{l-1}(\Omega_{s,j})$ for $s > 0$ if $j = -1$ and $s > 1$ if $j = 1$;

4. $\psi_l(\Gamma_{0,\lambda}) = \psi_{l-1}(\Gamma_{0,\lambda})^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(\Gamma_{1,\lambda}) + \psi_{l-1}(x_l)^{2(r-1)}\psi_{l-1}(\Gamma_{0,\lambda});$
5. $\psi_l(\Gamma_{1,\lambda}) = \psi_{l-1}(\Gamma_{1,\lambda})^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(\Gamma_{2,\lambda}) - 2\psi_{l-1}(x_l)^{r(r-1)}\psi_{l-1}(\Gamma_{0,\lambda})^r + \psi_{l-1}(x_l)^{(r+1)(r-1)}\psi_{l-1}(\Gamma_{1,\lambda});$
6. $\psi_l(\Gamma_{s,\lambda}) = \psi_{l-1}(\Gamma_{s,\lambda})^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(\Gamma_{s+1,\lambda}) - \psi_{l-1}(x_l)^{r^s(r-1)}\psi_{l-1}(\Gamma_{s-1,\lambda})^r + \psi_{l-1}(x_l)^{(r^s+1)(r-1)}\psi_{l-1}(\Gamma_{s,\lambda})$ for $s \geq 2$;
7. $\psi_l(\Lambda_{1,\lambda}) = \psi_{l-1}(\Lambda_{1,\lambda})^{q^2} - \psi_{l-1}(x_l)^{q^2-1}\psi_{l-1}(\Lambda_{2,\lambda}) - \psi_{l-1}(x_l)^{q^3-q}\psi_{l-1}(\Lambda_{1,\lambda})^q + \psi_{l-1}(x_l)^{q^3+q^2-q-1}\psi_{l-1}(\Lambda_{1,\lambda});$
8. $\psi_l(\Lambda_{s,\lambda}) = \psi_{l-1}(\Lambda_{s,\lambda})^{q^2} - \psi_{l-1}(x_l)^{q^2-1}\psi_{l-1}(\Lambda_{s+1,\lambda}) - \psi_{l-1}(x_l)^{q^{2s-1}(q^2-1)}\psi_{l-1}(\Lambda_{s-1,\lambda})^{q^2} + \psi_{l-1}(x_l)^{(q^{2s-1}+1)(q^2-1)}\psi_{l-1}(\Lambda_{s,\lambda})$ for $s \geq 2$.

Proof: We only prove 1, 2 and 3. All the other statements can be proved by similar calculations. But we should remember that when we consider the polynomials $\Lambda_{s,\lambda}$, r is equal to q^2 .

According to Proposition 3.1-3, the \mathbb{F} -algebra homomorphism ψ_l satisfies $\psi_l(x_i) = \psi_{l-1}(x_i)^r - \psi_{l-1}(x_l)^{r-1}\psi_{l-1}(x_i)$ for all i . For simplicity, let $T = \psi_{l-1}(x_l)$. Then

$$\psi_l(x_i) = \psi_{l-1}(x_i)^r - T^{r-1}\psi_{l-1}(x_i)$$

and

$$\begin{aligned} \psi_l(\Omega_{0,1}) &= \sum_{i=1}^m \psi_l(x_{n-i+1})\psi_l(x_i) \\ &= \sum_{i=1}^m (\psi_{l-1}(x_{n-i+1})^r - T^{r-1}\psi_{l-1}(x_{n-i+1}))(\psi_{l-1}(x_i)^r - T^{r-1}\psi_{l-1}(x_i)) \\ &= \psi_{l-1}(\Omega_{0,1})^r - T^{r-1}\psi_{l-1}(\Omega_{1,1}) + T^{2(r-1)}\psi_{l-1}(\Omega_{0,1}) \end{aligned}$$

which proves 1. Since

$$\begin{aligned}
\psi_l(\Omega_{s,j}) &= \sum_{i=1}^m (\psi_l(x_{n-i+1})^{r^s} \psi_l(x_i) + j \psi_l(x_{n-i+1}) \psi_l(x_i)^{r^s}) \\
&= \sum_{i=1}^m (\psi_{l-1}(x_{n-i+1})^{r^{s+1}} - T^{r^s(r-1)} \psi_{l-1}(x_{n-i+1})^{r^s}) (\psi_{l-1}(x_i)^r - T^{r-1} \psi_{l-1}(x_i)) \\
&\quad + j \sum_{i=1}^m (\psi_{l-1}(x_{n-i+1})^r - T^{r-1} \psi_{l-1}(x_{n-i+1})) (\psi_{l-1}(x_i)^{r^{s+1}} - T^{r^s(r-1)} \psi_{l-1}(x_i)^{r^s}),
\end{aligned}$$

2 and 3 follow easily. \square

Corollary 3.5 *Assume by convention that $\Omega_{s,j} = 0$, $\Gamma_{s,\lambda} = 0$ for $s < 0$ and $\Lambda_s = 0$ for $s \leq 0$. Then:*

1. $\psi_l(\Omega_{s,j}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-1}(x_l), \Omega_{s-1,j}, \Omega_{s,j}, \Omega_{s+1,j}, \dots, \Omega_{s+l,j}]$;
2. $\psi_l(\Gamma_{s,\lambda}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-1}(x_l), \Gamma_{s-1,\lambda}, \Gamma_{s,\lambda}, \Gamma_{s+1,\lambda}, \dots, \Gamma_{s+l,\lambda}]$;
3. $\psi_l(\Lambda_{s,\lambda}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-1}(x_l), \Lambda_{s-1,\lambda}, \Lambda_{s,\lambda}, \Lambda_{s+1,\lambda}, \dots, \Lambda_{s+l,\lambda}]$

Proof: We only prove the statement in 1. We do this by induction on l . For $l = 1$, it follows from Proposition 3.4-3 that

$$\psi_1(\Omega_{s,j}) = \Omega_{s,j}^r - x_1^{r-1} \Omega_{s+1,j} - x_1^{r^s(r-1)} \Omega_{s-1,j}^r + x_1^{(r^s+1)(r-1)} \Omega_{s,j} \in \mathbb{F}[x_1, \Omega_{s-1,j}, \Omega_{s,j}, \Omega_{s+1,j}].$$

Now, assume that the result is true for $l - 1$. Again from Proposition 3.4-1,2,3 we get

$$\begin{aligned}
\psi_l(\Omega_{s,j}) &= \psi_{l-1}(\Omega_{s,j})^r - \psi_{l-1}(x_l)^{r-1} \psi_{l-1}(\Omega_{s+1,j}) - \psi_{l-1}(x_l)^{r^s(r-1)} \psi_{l-1}(\Omega_{s-1,j})^r \\
&\quad + \psi_{l-1}(x_l)^{(r^s+1)(r-1)} \psi_{l-1}(\Omega_{s,j}).
\end{aligned}$$

By induction we have

- $\psi_{l-1}(\Omega_{s,j}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-2}(x_{l-1}), \Omega_{s-1,j}, \Omega_{s,j}, \Omega_{s+1,j}, \dots, \Omega_{s+l-1,j}]$;
- $\psi_{l-1}(\Omega_{s+1,j}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-2}(x_{l-1}), \Omega_{s,j}, \Omega_{s+1,j}, \dots, \Omega_{s+l,j}]$;

- $\psi_{l-1}(\Omega_{s-1,j}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-2}(x_{l-1}), \Omega_{s-2,j}, \Omega_{s-1,j}, \Omega_{s,j}, \dots, \Omega_{s+l-2,j}]$ if $s - 1 > 0$.

Hence,

$$\psi_l(\Omega_{s,j}) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-1}(x_l), \Omega_{s-1,j}, \Omega_{s,j}, \Omega_{s+1,j}, \dots, \Omega_{s+l,j}].$$

Similarly, the other statements can be obtained also by induction on l . \square

Proposition 3.6 *For every $l \geq 0$ and $s > 0$, the polynomials $\psi_l(\Omega_{0,1})$, $\psi_l(\Omega_{s,j})$, $\psi_l(\Gamma_{0,\lambda})$, $\psi_l(\Gamma_{s,\lambda})$ and $\psi_l(\Lambda_{s,\lambda})$ belong to $\mathbb{F}[x_1, \dots, x_{n-l}]$. Moreover, for $0 \leq l \leq m - 1$, their degree in the variable x_{n-l} is:*

1. r^l for $\psi_l(\Omega_{0,1})$ and $\psi_l(\Gamma_{0,\lambda})$;
2. r^{l+s} for $\psi_l(\Omega_{s,j})$ and $\psi_l(\Gamma_{s,\lambda})$;
3. $q^{2l+2s-1}$ for $\psi_l(\Lambda_{s,\lambda})$.

Proof: Since $\psi_l(x_i) = 0$ for all $i \leq l$, it is easy to see that $\psi_l(\Omega_{0,1}), \psi_l(\Omega_{s,j}), \psi_l(\Gamma_{0,\lambda}), \psi_l(\Gamma_{s,\lambda}), \psi_l(\Lambda_{s,\lambda}) \in \mathbb{F}[x_1, \dots, x_{n-l}]$.

By definition $\psi_l(x_i) = F_{l,r}(x_i)$ and it can be easily proven by induction on l that $F_{l,r}(x_i) \in \mathbb{F}[x_1, \dots, x_i]$ with degree r^l in x_i . Since

$$\psi_l(\Omega_{0,1}) = \sum_{i=l+1}^m \psi_l(x_{n-i+1})\psi_l(x_i)$$

we conclude that $\psi_l(\Omega_{0,1})$ and $\psi_l(\Gamma_{0,\lambda})$ have degree r^l in x_{n-l} for $0 \leq l \leq m - 1$. For $\Omega_{s,j}$, we have

$$\psi_l(\Omega_{s,j}) = \sum_{i=l+1}^m \psi_l(x_{n-i+1})^{r^s} \psi_l(x_i) + j\psi_l(x_{n-i+1})\psi_l(x_i)^{r^s}$$

and therefore $\psi_l(\Omega_{s,j})$ has degree r^{l+s} in x_{n-l} . Similar arguments give us the results for $\psi_l(\Gamma_{s,\lambda})$ and $\psi_l(\Lambda_{s,\lambda})$. \square

We finish this section by studying the invariant rings for a family of subgroups of $U(n, \mathbb{F})$. We start with an example to illustrate what is our goal and how we shall proceed to achieve it.

Example 3.7 Consider the polynomial ring $\mathbb{F}_q[x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9]$ and let H denote the subgroup of $U(9, q)$ formed by the matrices

$$H_C = \left(\begin{array}{c|c|c} I_4 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline C & 0 & I_4 \end{array} \right)$$

where I_4 is the 4×4 identity matrix and C is a 4×4 matrix such that $c_{i,j} = c_{4-j+1, 4-i+1}$, i.e.,

$$C = \begin{pmatrix} c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} \\ c_{2,1} & c_{2,2} & c_{2,3} & c_{1,3} \\ c_{3,1} & c_{3,2} & c_{2,2} & c_{1,2} \\ c_{4,1} & c_{3,1} & c_{2,1} & c_{1,1} \end{pmatrix}$$

We want to determine a lower bound for the minimal degree in x_m of a polynomial in $\mathbb{F}_q[x_1, x_2, x_3, x_4, x_5, \dots, x_m]^H$ for each $m = 6, 7, 8, 9$.

We define $C^{(1)} = C$ and for $k = 2, 3, 4$, $C^{(k)}$ will be the matrix obtained from C by fixing all the entries of the first $k - 1$ rows equal to zero. For example,

$$C^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ c_{3,1} & c_{3,2} & 0 & 0 \\ c_{4,1} & c_{3,1} & 0 & 0 \end{pmatrix}.$$

For each k , take the set formed by the elements $H_{C^{(k)}}$. This is a subgroup of H which we will denote by L_k . Note that $L_1 = H$.

We write $P[k]$ for $\mathbb{F}_q[x_1, x_2, x_3, x_4, x_5, x_{5+1}, \dots, x_{5+k}]$. Then the groups L_k act on $P[k]$ by fixing $x_1, x_2, x_3, x_4, x_5, \dots, x_{5+k-1}$ and

$$x_{5+k} \mapsto x_{5+k} + \sum_{j=1}^{4-k+1} c_{k,j} x_j.$$

Therefore, L_k is acting like a subgroup of $U(5+k, q)$ with order q^{5-k} . The orbit product of x_{5+k} under L_k is

$$N(x_{5+k}) = F_{4-k,q}(x_{5+k})^q - F_{4-k,q}(x_{5-k})^{q-1} F_{4-k,q}(x_{5+k})$$

and has degree q^{5-k} . Hence

$$P[k]^{L_k} = \mathbb{F}_q[x_1, x_2, x_3, x_4, x_5, x_{5+1}, \dots, x_{5+k-1}, N(x_{5+k})].$$

Furthermore, if we consider the graded reverse lexicographic order with $x_9 > \dots > x_1$, then according to Corollary 2.36, $\{x_1, x_2, x_3, x_4, x_5, x_{5+1}, \dots, x_{5+k-1}, N(x_{5+k})\}$ is a SABGI basis for $P[k]^{L_k}$. Thus the degree in x_{5+k} of $N(x_{5+k})$ is minimal among the elements of $P[k]^{L_k}$.

Since for each k ,

$$P[k]^H \subset P[k]^{L_k}$$

we conclude that the minimal degree in x_{5+k} of a polynomial in $P[k]^H$ is greater than or equal to q^{5-k} .

Let H^+ be the set of matrices

$$\left(\begin{array}{c|c|c} I_t & 0 & 0 \\ \hline 0 & I_d & 0 \\ \hline C^+ & 0 & I_t \end{array} \right)$$

where I_t and I_d are the $t \times t$ and $d \times d$ identity matrices, respectively; and C^+ is any $t \times t$ matrix with entries in \mathbb{F} such that

$$c_{i,j}^+ = \bar{c}_{t-j+1, t-i+1}^+ \quad \text{for all } i \text{ and } j.$$

It is not hard to check that H^+ is an abelian subgroup of $U(2t+d, \mathbb{F})$. If in the elements of H^+ we replace the matrix C^+ by a matrix C^- , of the same dimension, such that

$$c_{i,j}^- = -\bar{c}_{t-j+1, t-i+1}^- \quad \text{for all } i \text{ and } j$$

we obtain another abelian subgroup of $U(2t+d, \mathbb{F})$. We denote it by H^- .

For any matrix A and $k \geq 1$ define:

- $A^{(1)} = A$;
- $A^{(k)}$ is the matrix obtained from A by fixing all the entries in the first $k-1$ rows equal to zero.

Now, we define a family of subgroups of H^+ and H^- . Let $k \in \{1, 2, \dots, t\}$. We represent by L_k^+ the subgroup of H^+ formed by the matrices

$$\left(\begin{array}{c|c|c} I_t & 0 & 0 \\ \hline 0 & I_d & 0 \\ \hline C^{+(k)} & 0 & I_t \end{array} \right).$$

Replacing $C^{+(k)}$ by $C^{-(k)}$ in the elements of L_k^+ , we obtain a subgroup of H^- which we represent by L_k^- .

Let $P[k]$ denote the polynomial ring $\mathbb{F}[x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k}]$. We want to determine the invariant rings $P[k]^{L_k^+}$ and $P[k]^{L_k^-}$ for all k . First, we need to see what happens to the entries of the matrices C^+ and C^- when we take different fields.

Lemma 3.8 *Consider the matrices C^+ and C^- . Then*

1. *For $\mathbb{F} = \mathbb{F}_{q^2}$, we obtain*

- $c_{i, t-i+1}^+ \in \mathbb{F}_q$ for all i and $c_{i,j}^+ \in \mathbb{F}_{q^2}$ if $j \neq t-i+1$.
- $c_{i, t-i+1}^- + \bar{c}_{i, t-i+1}^- = 0$ for all i and $c_{i,j}^- \in \mathbb{F}_{q^2}$ if $j \neq t-i+1$.

2. For $\mathbb{F} = \mathbb{F}_q$, we get

- $c_{i,j}^+ \in \mathbb{F}_q$ for all i and j .
- If q is odd then $c_{i,t-i+1}^- = 0$ for all i and if q is even then $c_{i,j}^- \in \mathbb{F}_q$ for all i and j .

Proof: All the statements follow from the fact that $c_{i,j}^+ = \bar{c}_{i,j}^+$ if and only if

$$\begin{cases} t - i + 1 = j \\ t - j + 1 = i \end{cases} \iff \begin{cases} j = t - i + 1 \\ i = i \end{cases}.$$

And the same is true if we take C^- instead. \square

Proposition 3.9 *Let $k \in \{1, \dots, t\}$. Then*

$$P[k]^{L_k^+} = \mathbb{F}[x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k-1}, N(x_{t+d+k})]$$

where $N(x_{t+d+k})$ is the orbit product of x_{t+d+k} and in this variable its degree is:

- $q^{2(t-k)+1}$ if $\mathbb{F} = \mathbb{F}_{q^2}$,
- q^{t-k+1} if $\mathbb{F} = \mathbb{F}_q$.

Moreover, in the graded reverse lexicographic order with $x_{t+d+k} > \dots > x_1$ this set of generators for $P[k]^{L_k^+}$ is a SABGI basis.

Proof: For each k , the group L_k^+ acts on $P[k]$ in the following way: it fixes x_i for all $i \leq t + d + k - 1$ and

$$x_{t+d+k} \mapsto x_{t+d+k} + \sum_{j=1}^{t-k+1} c_{k,j}^+ x_j.$$

Note that this defines an action of a subgroup L of $U(t+d+k, \mathbb{F})$. Thus $P[k]^{L_k^+} = P[k]^L$.

We will show that the product of the degrees of $x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k-1}$, and $N(x_{t+d+k})$ is equal to the order of L , which is the same as showing that the degree of $N(x_{t+d+k})$ equals the order of L . Therefore, applying Theorem 2.5 we will obtain

$$P[k]^L = \mathbb{F}[x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k-1}, N(x_{t+d+k})].$$

First, we consider $\mathbb{F} = \mathbb{F}_{q^2}$. Applying Lemma 3.8-1 we can conclude that the order of L is $q^{2(t-k)+1}$. By Lemma 2.28-1,

$$N(x_{t+d+k}) = F_{t-k,q^2}(x_{t+d+k})^q - F_{t-k,q^2}(x_{t-k+1})^{q-1} F_{t-k,q^2}(x_{t+d+k})$$

and has degree $q^{2(t-k)+1}$. Now, when $\mathbb{F} = \mathbb{F}_q$, the group L has order q^{t-k+1} by Lemma 3.8-2. In this case

$$\begin{aligned} N(x_{t+d+k}) &= \prod_{c_{k,1}^+ \dots c_{k,t-k+1}^+ \in \mathbb{F}_q} x_{t+d+k} + \sum_{j=1}^{t-k+1} c_{k,j}^+ x_j \\ &= F_{t-k,q}(x_{t+d+k})^q - F_{t-k,q}(x_{t-k+1})^{q-1} F_{t-k,q}(x_{t+d+k}) \end{aligned}$$

and its order is q^{t-k+1} .

For the second part, we can easily see that in the graded reverse lexicographic order, with $x_{t+d+k} > \dots > x_1$, the leading monomial of $N(x_{t+d+k})$ is x_{t+d+k}^d with $d = q^{2(t-k)+1}$ if $\mathbb{F} = \mathbb{F}_{q^2}$ or $d = q^{t-k+1}$ if $\mathbb{F} = \mathbb{F}_q$. In both cases applying Corollary 2.36 we conclude that $\{x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k-1}, N(x_{t+d+k})\}$ is a *SAGBI* basis for $P[k]^{L_k^+}$. \square

We have a similar proposition for the groups L_k^- .

Proposition 3.10 *Let $k \in \{1, \dots, t\}$. Then*

$$P[k]^{L_k^-} = \mathbb{F}[x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k-1}, N(x_{t+d+k})]$$

where $N(x_{t+d+k})$ is the orbit product of x_{t+d+k} and in this variable it has degree:

- $q^{2(t-k)+1}$ if $\mathbb{F} = \mathbb{F}_{q^2}$,
- q^{t-k} if $\mathbb{F} = \mathbb{F}_q$ and q is odd,
- q^{t-k+1} if $\mathbb{F} = \mathbb{F}_q$ and q is even.

Moreover, in the graded reverse lexicographic order with $x_{t+d+k} > \dots > x_1$ this set of generators for $P[k]^{L_k^-}$ is a *SABGI* basis.

Proof: Just as in the proof of Proposition 3.9, the action of L_k^- also defines an action of a subgroup L of $U(t+d+k, \mathbb{F})$ on $P[k]$ and we just need to show that the degree of $N(x_{t+d+k})$ is equal to the order of L .

When $\mathbb{F} = \mathbb{F}_{q^2}$ it follows from Lemma 3.8-1 that L has order $q^{2(t-k)+1}$ and from Lemma 2.28-2 that

$$N(x_{t+d+k}) = F_{t-k, q^2}(x_{t+d+k})^q + F_{t-k, q^2}(x_{t-k+1})^{q-1} F_{t-k, q^2}(x_{t+d+k})$$

has degree $q^{2(t-k)+1}$. For $\mathbb{F} = \mathbb{F}_q$, we just apply Lemma 3.8-2 to obtain that the order of L is q^{t-k} if q is odd and q^{t-k+1} if q is even. In each case, the calculation of $N(x_{t+d+k})$ and its degree is straightforward.

Again, like in the proof of Proposition 3.9, we apply Corollary 2.36 to show that $\{x_1, \dots, x_{t+d}, x_{t+d+1}, \dots, x_{t+d+k-1}, N(x_{t+d+k})\}$ is a *SAGBI* basis for $P[k]^{L_k^-}$. \square

Finally, we can determine a lower bound for the minimal degree in x_{t+d+k} of a polynomial in $P[k]^{H^+}$ and also of a polynomial in $P[k]^{H^-}$.

Proposition 3.11 *Let $k \in \{1, \dots, t\}$. Then the minimal degree in x_{t+d+k} of:*

1. *a polynomial in $P[k]^{H^+}$ is greater than or equal to*

$$\begin{cases} q^{2(t-k)+1} & \text{if } \mathbb{F} = \mathbb{F}_{q^2} \\ q^{t-k+1} & \text{if } \mathbb{F} = \mathbb{F}_q \end{cases}.$$

2. *a polynomial in $P[k]^{H^-}$ is greater than or equal to*

$$\begin{cases} q^{2(t-k)+1} & \text{if } \mathbb{F} = \mathbb{F}_{q^2} \\ q^{t-k} & \text{if } \mathbb{F} = \mathbb{F}_q \text{ and } q \text{ odd} \\ q^{t-k+1} & \text{if } \mathbb{F} = \mathbb{F}_q \text{ and } q \text{ even} \end{cases}.$$

Proof: It follows from Propositions 3.9 and 3.10 that the degree of $N(x_{t+d+k})$ is the minimal degree in x_{t+d+k} of a polynomial in $P[k]^{L_k^+}$ or $P[k]^{L_k^-}$. Since for each k we have

$$P[k]^{H^+} \subset P[k]^{L_k^+} \quad \text{and} \quad P[k]^{H^-} \subset P[k]^{L_k^-},$$

applying Propositions 3.9 and 3.10 completes the proof. \square

Remark 3.12 *It follows from the proof of Proposition 3.10 that if $\mathbb{F} = \mathbb{F}_q$ with q even and if all the matrices C^- also satisfy $c_{i,t-i+1}^- = 0$ for every i , then the orbit product $N(x_{t+d+k})$ has degree q^{t-k} in x_{t+d+k} . In this case the minimal degree in x_{t+d+k} of a polynomial in $P[k]^{H^-}$ will be greater than or equal to q^{t-k} .*

We finish this section by studying the invariant ring for two different subgroups of $U(n, \mathbb{F})$. So let

- U_1 be the set of elements $u \in U(n, \mathbb{F})$ such that $u(x_j) = x_j + \sum_{k=1}^{j-1} a_{jk}x_k$, for $1 \leq j \leq n-1$ and $u(x_n) = x_n + \sum_{k=1}^{n-2} a_{jk}x_k$;
- U_2 be the set of elements $u \in U(n, \mathbb{F}_{q^2})$ such that $u(x_j) = x_j + \sum_{k=1}^{j-1} a_{jk}x_k$, for $1 \leq j \leq n-1$ and $u(x_n) = x_n + bx_{n-1} + \sum_{k=1}^{n-2} a_{jk}x_k$ with $b + \bar{b} = 0$.

Lemma 3.13 *Let U_1 and U_2 be the groups above defined. For each $j \in \{1, \dots, n\}$ and $k \in \{1, 2\}$ we have*

$$\mathbb{F}[x_1, x_2, \dots, x_j]^{U_k} = \mathbb{F}[x_1, N(x_2), \dots, N(x_j)]$$

where $N(x_i)$ is the orbit product of x_i for $i \leq j$. Furthermore, the degree in x_j of $N(x_j)$ is minimal among the elements in $\mathbb{F}[x_1, x_2, \dots, x_j]^{U_k}$.

Proof: The groups U_k act on $\mathbb{F}[x_1, x_2, \dots, x_{n-1}]$ in the same way as $U(n-1, \mathbb{F})$. Hence, it follows from Example 2.27 that

$$\mathbb{F}[x_1, x_2, \dots, x_{n-1}]^{U_k} = \mathbb{F}[x_1, N(x_2), \dots, N(x_{n-1})].$$

Now the order of U_k is $|U(n-1, \mathbb{F})|s$. We will show that the degree of $N(x_n)$ is equal to s and then we apply Theorem 2.5.

Let r be the number of elements in \mathbb{F} . First, we consider the group U_1 . Therefore $s = r^{n-2}$. It is not hard to see that $N(x_n) = F_{n-2,r}(x_n)$ and consequently its degree is

r^{n-2} . For the group U_2 , $s = q^{2(n-2)}q$ which is the degree of $N(x_n)$ according to Lemma 2.28-2.

Now, we prove the second part of this Lemma. Note that if we consider for each $1 \leq j \leq m+1$ the graded reverse lexicographic order with $x_j > \cdots > x_1$, then the leading monomials of $N(x_i)$ are of the form $x_i^{d_i}$ for all $i \leq j$. Applying Corollary 2.36 we conclude that $\{x_1, N(x_2), \dots, N(x_j)\}$ is a *SAGBI* basis for $\mathbb{F}[x_1, x_2, \dots, x_j]^{U_k}$ and so the degree of $N(x_j)$ is minimal among the elements of $\mathbb{F}[x_1, x_2, \dots, x_j]^{U_k}$. \square

3.2 The Invariant Field of a Sylow p -subgroup of $GU(2m, q^2)$

Let G denote the Sylow p -subgroup of $GU(2m, q^2)$ given by Proposition 1.24. Also, recall from Section 2.3 that $R[j] = \mathbb{F}_{q^2}[x_1, \dots, x_j]$ for $1 \leq j \leq 2m$ and ϕ_j is an element of $R[j]^G$ with the smallest degree in x_j .

First, we introduce a family of polynomials which we shall prove to be invariants under the action of G . For $k \geq 1$ define

$$h_k := \Lambda_{k,0}.$$

Thus $h_1 = \sum_{i=1}^m (x_{2m-i+1}^q x_i + x_{2m-i+1} x_i^q)$.

Lemma 3.14 *For all $k \geq 1$ the polynomials h_k belong to $\mathbb{F}_{q^2}[V]^{GU(2m, q^2)}$.*

Proof: From Corollary 3.3 we get $h_k = \mathcal{P}^{q^{2k-3}}(h_{k-1})$ for $k > 1$, where $\mathcal{P}^{q^{2k-3}}$ is the q^{2k-3} -th Steenrod operation. Hence it is enough to prove that h_1 is an invariant polynomial.

Take $v \in \bar{V} = \bar{\mathbb{F}}_{q^2} \otimes_{\mathbb{F}_{q^2}} V$, where $\bar{\mathbb{F}}_{q^2}$ is the algebraic closure of \mathbb{F}_{q^2} . Thus

$$h_1(v) = \sum_{i=1}^m (\alpha_{2m-i+1}^q \alpha_i + \alpha_{2m-i+1} \alpha_i^q)$$

where $v = \sum_{i=1}^m (\alpha_{2m-i+1}u_i + \alpha_i v_i)$. If we take $X = [\alpha_1, \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_{2m}]^T$ and J_{2m} the matrix given by 1.5, then

$$h_1(v) = X^T J_{2m} \bar{X}.$$

Now, let $M \in GU(2m, q^2)$ and $Y = M^{-1}X$. Then $M.h_1 = h_1$ since

$$(M.h_1)(v) = h_1(M^{-1}v) = Y^T J_{2m} \bar{Y} = X^T (M^{-1})^T J_{2m} \bar{M}^{-1} \bar{X} = X^T J_{2m} \bar{X} = h_1(v),$$

where we have used the definition of $GU(2m, q^2)$, i.e., $M^T J_{2m} \bar{M} = J_{2m}$. \square

Let $N(x_i)$ be the orbit product of x_i under the action of G for all i .

Theorem 3.15 *The invariant field $\mathbb{F}_{q^2}(V)^G$ is generated by the polynomials $N(x_j)$, with $j = 1, \dots, m+1$, and the polynomials h_k , with $k = 1, \dots, m-1$, i.e.,*

$$\mathbb{F}_{q^2}(V)^G = \mathbb{F}_{q^2}(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1}).$$

Proof: We shall use Theorem 2.23 to get the result. We start by noting that the matrices F in the elements of G look like

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

where c is an element in \mathbb{F}_{q^2} satisfying $c + \bar{c} = 0$. Hence G acts on $R[m+1]$ in the same way as the group U_2 in Lemma 3.13 and so $R[j]^G = R[j]^{U_2}$ for each $j \in \{1, \dots, m+1\}$. It also follows from Lemma 3.13 that $N(x_j)$ is an element in $R[j]^G$ of minimal degree in x_j . Therefore, for each $j \in \{1, \dots, m+1\}$ we choose $\phi_j = N(x_j)$.

Now, if we consider all the elements of G for which A and F are the identity matrices and B the zero matrix, then we obtain an abelian subgroup H of G whose elements are

$$\left(\begin{array}{c|c|c} I_{m-1} & 0 & 0 \\ \hline 0 & I_2 & 0 \\ \hline J_{m-1} \bar{S} & 0 & I_{m-1} \end{array} \right)$$

with $S \in M(m-1, q^2)$ such that $S + \bar{S}^T = 0$ and J_{m-1} is the matrix given by (1.5).

Let $C = J_{m-1}\bar{S}$. Note that the multiplication by J_{m-1} swaps the rows i and $(m-1) - i + 1 = m - i$ of \bar{S} for all i . Thus, since $S + \bar{S}^T = 0$ we obtain

$$c_{i,j} = \bar{s}_{m-i,j} = -s_{j,m-i} = -\bar{c}_{m-j,m-i}.$$

Now, assume that C is a $(m-1) \times (m-1)$ matrix with entries in \mathbb{F}_{q^2} such that

$$c_{i,j} = -\bar{c}_{(m-1)-j+1,(m-1)-i+1} = -\bar{c}_{m-j,m-i}.$$

By taking $S = J_{m-1}\bar{C}$ we get

$$s_{i,j} = -\bar{c}_{m-i,j} = -c_{m-j,i} = -\bar{s}_{j,i}$$

and therefore $S + \bar{S}^T = 0$. Hence H is the subgroup H^- from Section 3.1 with $t = m-1$ and $d = 2$.

Let $l \in \{0, \dots, m-2\}$. Using the results of Section 3.1 we can compute the polynomials ϕ_{2m-l} in $R[2m-l]^G$ of minimal degree in x_{2m-l} . Since

$$R[2m-l]^G \subset R[2m-l]^H = P[m-l-1]^{H^-},$$

applying Proposition 3.11 we obtain that the minimal degree in x_{2m-l} of an element in $R[2m-l]^G$ is greater than or equal to q^{2l+1} . By Proposition 3.6 this is the degree of

$$\psi_l(\Lambda_{1,0}) = \psi_l(h_1).$$

Now, if we can show that $\psi_l(h_1) \in R[2m-l]^G$, then we can take $\phi_{2m-l} = \psi_l(h_1)$.

Applying Corollary 3.5 and using the definition of h_k we get

$$\psi_l(h_1) \in \mathbb{F}_{q^2}[x_1, \psi_1(x_2), \dots, \psi_{l-1}(x_l), h_1, h_2, \dots, h_{l+1}], \quad (3.1)$$

which is a subalgebra of $R[2m-l]^G$ by Proposition 3.1-2 and Lemma 3.14. it follows from Theorem 2.23 that

$$\mathbb{F}_{q^2}(V)^G = \mathbb{F}_{q^2}(x_1, N(x_2), \dots, N(x_{m+1}), \psi_{m-2}(h_1), \dots, \psi_1(h_1), h_1).$$

Finally, using 3.1 we obtain

$$\mathbb{F}_{q^2}(V)^G = \mathbb{F}_{q^2}(x_1, N(x_2), \dots, N(x_{m+1}), h_{m-1}, \dots, h_1)$$

and this finishes the proof. \square

3.3 The Invariant Field of a Sylow p -subgroup of $GU(2m+1, q^2)$

Let G denote the Sylow p -subgroup of $GU(2m+1, q^2)$ given by Proposition 1.25.

We consider the following family of polynomials: for $k \geq 1$ let

$$h_k := \Lambda_{k,1}.$$

Thus $h_1 = \sum_{i=1}^m (x_{2m+1-i+1}^q x_i + x_{2m+1-i+1} x_i^q) + x_{m+1}^{q+1}$.

Lemma 3.16 *For all $k \geq 1$ the polynomials h_k belong to $\mathbb{F}_{q^2}[V]^{GU(2m+1, q^2)}$.*

Proof: From Corollary 3.3 we get $h_k = \mathcal{P}^{q^{2k-3}}(h_{k-1})$ for $k > 1$. Hence it suffices to prove that h_1 is invariant. We follow the same steps as in the proof of Lemma 3.14. Just note that in this case

$$h_1(v) = X^T \left(\begin{array}{c|c|c} 0 & 0 & J_m \\ \hline 0 & 1 & 0 \\ \hline J_m & 0 & 0 \end{array} \right) \bar{X},$$

with $X = [\alpha_1, \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_{2m+1}]^T$. \square

We denote by $N(x_i)$ the orbit product of x_i under the action of G for all i .

Theorem 3.17 *The invariant field $\mathbb{F}_{q^2}(V)^G$ is generated by the polynomials $N(x_j)$, with $j = 1, \dots, m+1$, and the polynomials h_k , with $k = 1, \dots, m$, i.e.,*

$$\mathbb{F}_{q^2}(V)^G = \mathbb{F}_{q^2}(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_m).$$

Proof: In this case G acts on $R[m+1]$ like the group $U(m+1, q^2)$. Therefore, for each $j \in \{1, \dots, m+1\}$, the degree in x_j of $N(x_j) \in R[j]^G$ is minimal and we can take $\phi_j = N(x_j)$.

If we consider the elements of G for which A is the identity matrix and v is the zero vector, then we obtain an abelian subgroup H with elements

$$\left(\begin{array}{c|c|c} I_m & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline J_m \bar{S} & 0 & I_{m-1} \end{array} \right)$$

where $S \in M(m, q^2)$ is such that $S + \bar{S}^T = 0$. Similarly to what was done in the proof of Theorem 3.15, we can show that H is the group H^- of Section 3.1 with $t = m$ and $d = 1$.

Let $l \in \{0, \dots, m-1\}$. Since

$$R[2m+1-l]^G \subset R[2m+1-l]^H = P[m-l]^{H^-}$$

and using Proposition 3.11, we can see that the minimal degree in x_{2m+1-l} of a polynomial in $R[2m+1-l]^G$ is greater than or equal to q^{2l+1} . By Proposition 3.6, this is the degree of

$$\psi_l(\Lambda_{1,1}) = \psi_l(h_1).$$

Now, from Corollary 3.5, Proposition 3.1-2 and the definition of h_k it follows that

$$\psi_l(h_1) \in \mathbb{F}_{q^2}[x_1, N(x_2), \dots, N(x_l), h_1, h_2, \dots, h_{l+1}].$$

Then according to Lemma 3.16 we have $\psi_l(h_1) \in R[2m+1-l]^G$ and therefore we can take $\phi_{2m+1-l} = \psi_l(h_1)$.

Finally, applying Theorem 2.23 we conclude that

$$\mathbb{F}_{q^2}(V)^G = \mathbb{F}_{q^2}(x_1, N(x_2), \dots, N(x_{m+1}), h_m, \dots, h_1)$$

and this finishes the proof. \square

3.4 The Invariant Field of a Sylow p -subgroup of $Sp(2m, q)$

Let G be the Sylow p -subgroup of $Sp(2m, q)$ given by Proposition 1.27. Now, for each $k \geq 1$ let

$$h_k := \Omega_{k,-1}.$$

Therefore $h_1 = \sum_{i=1}^m (x_{2m-i+1}^q x_i - x_{2m-i+1} x_i^q)$. The next lemma shows that, in particular, h_k is invariant under the action of G for all k .

Lemma 3.18 *For all $k \geq 1$ the polynomials h_k belong to $\mathbb{F}_q[V]^{Sp(2m, q)}$.*

Proof: By Corollary 3.3, $h_k = \mathcal{P}^{q^{k-1}}(h_{k-1})$ for $k > 1$ and so it is enough to prove that h_1 is an invariant polynomial.

Let $v \in \bar{V} = \bar{\mathbb{F}}_q \otimes_{\mathbb{F}_q} V$, where $\bar{\mathbb{F}}_q$ is the algebraic closure of \mathbb{F}_q . Thus

$$h_1(v) = \sum_{i=1}^m (\alpha_{2m-i+1}^q \alpha_i - \alpha_{2m-i+1} \alpha_i^q)$$

where $v = \sum_{i=1}^m (\alpha_{2m-i+1} u_i + \alpha_i v_i)$. If we take $X = [\alpha_1, \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_{2m}]^T$, J_{m-1} the matrix given by (1.5),

$$J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } Q_{2m} := \left(\begin{array}{c|c|c} 0 & 0 & J_{m-1} \\ \hline 0 & J & 0 \\ \hline -J_{m-1} & 0 & 0 \end{array} \right)$$

then

$$h_1(v) = X^T Q_{2m} \bar{X}.$$

Let $M \in Sp(2m, q)$ and $Y = M^{-1}X$. Since M satisfies $M^T Q_{2m} M = Q_{2m}$ and $\bar{M} = M$ we obtain

$$(M.h_1)(v) = h_1(M^{-1}v) = X^T (M^{-1})^T Q_{2m} \bar{M}^{-1} \bar{X} = X^T Q_{2m} \bar{X} = h_1(v),$$

Hence $M.h_1 = h_1$, i.e. h_1 is invariant. \square

Let $N(x_i)$ be the orbit product of x_i under the action of G for all i .

Theorem 3.19 *The invariant field $\mathbb{F}_q(V)^G$ is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m+1$, and the polynomials h_k , with $k = 1, \dots, m-1$, i.e.,*

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1}).$$

Proof: By choosing the elements of G for which A and F are the identity matrices and B is the zero matrix, we obtain an abelian subgroup H of G with elements

$$\left(\begin{array}{c|c|c} I_{m-1} & 0 & 0 \\ \hline 0 & I_2 & 0 \\ \hline J_{m-1}S & 0 & I_{m-1} \end{array} \right)$$

where $S \in M(m-1, q)$ is such that $S - S^T = 0$. It is easy to check that if $C = J_{m-1}S$ then $c_{i,j} = c_{m-j, m-i}$. Also if C is any matrix with entries in \mathbb{F}_q satisfying $c_{i,j} = c_{m-j, m-i}$ then $S = J_{m-1}C$ satisfies $S - S^T = 0$. Hence H is in fact the group H^+ Section 3.1 with $t = m-1$ and $d = 2$.

Let $l \in \{0, \dots, m-2\}$. Since

$$R[2m-l]^G \subset R[2m-l]^H = P[m-l-1]^{H^+}$$

the minimal degree in x_{2m-l} of a polynomial in $R[2m-l]^G$ is, according to Proposition 3.11, greater than or equal to q^{l+1} . We know from Proposition 3.6 that q^{l+1} is actually the degree of

$$\psi_l(\Omega_{1,-1}) = \psi_l(h_1).$$

It follows from Corollary 3.5 and the definition of h_k that

$$\psi_l(h_1) \in \mathbb{F}[x_1, \psi_1(x_2), \dots, \psi_{l-1}(x_l), h_1, h_2, \dots, h_l].$$

Therefore, $\psi_l(h_1)$ is an invariant polynomial by Proposition 3.1-2 and Lemma 3.18. Hence we can take $\phi_{2m-l} = \psi_l(h_1)$ for each $l \in \{0, \dots, m-1\}$.

Finally for each $j \in \{1, \dots, m+1\}$, we compute the polynomial ϕ_j . We note that G is acting on $R[m+1]$ in the same way as is the group $U(m+1, \mathbb{F}_q)$. Hence $R[j]^G = R[j]^U$

and therefore we can choose $\phi_j = N(x_j)$. Applying Theorem 2.23 we conclude that

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_m, \dots, h_1)$$

and this finishes the proof. \square

3.5 The Invariant Field of a Sylow p -subgroup of $O^+(2m, q)$

Recall from Section 1.6 the definition $O^+(2m, q)$. According to Proposition 1.33 it is group of invertible matrices that preserve the quadratic form

$$Q(v) = \sum_{i=1}^m \alpha_{2m-i+1} \alpha_i$$

with $v = \sum_{i=1}^m (\alpha_i u_i + \alpha_{2m-i+1} v_i)$.

Now consider the following family of polynomials: for $k \geq 1$ define

$$h_k := \Omega_{k-1,1}.$$

In particular, $h_1 = \sum_{i=1}^m x_{2m-i+1} x_i$. The next lemma shows that h_k is invariant under the action of $O^+(2m, q)$ for all k .

Lemma 3.20 *For all $k \geq 1$ the polynomials h_k belong to $\mathbb{F}_q[V]^{O^+(2m, q)}$.*

Proof: We know from Corollary 3.3 that for $k > 1$, h_k is the q^{k-2} -th Steenrod operation of h_{k-1} and therefore we just have to show that h_1 is invariant. This follows directly from the definition of the group $O^+(2m, q)$. In fact, for $v \in V$ we have $h_1(v) = Q(v)$ and so if $M \in O^+(2m, q)$ then

$$M.h_1(v) = h_1(M^{-1}v) = Q(M^{-1}v) = Q(v) = h_1(v).$$

Hence h_1 is invariant. \square

We have to consider separately the cases when the characteristic of \mathbb{F}_q is 2 and when it is not.

First, assume that the characteristic is not 2 and let G be the Sylow p -subgroup of $O^+(2m, q)$ given by Proposition 1.35. We represent by $N(x_i)$ the orbit product of x_i under the action of G for all i .

Theorem 3.21 *The invariant field $\mathbb{F}_q(V)^G$ is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m+1$, and the polynomials h_k , with $k = 1, \dots, m-1$, i.e.,*

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1}).$$

Proof: First let us consider the abelian subgroup H of G obtained by taking the elements of G for which the matrices A and B are equal to the identity and the zero matrix, respectively. Thus an element in H is of the form

$$\left(\begin{array}{c|c|c} I_{m-1} & 0 & 0 \\ \hline 0 & I_2 & 0 \\ \hline J_{m-1}S & 0 & I_{m-1} \end{array} \right)$$

where $S \in M(m-1, q)$ is such that $S + S^T = 0$. Analogously to what was done in the proofs of Theorems 3.15 and 3.19, we can easily show that H is the subgroup H^- defined in Section 3.1 with $t = m-1$ and $d = 2$.

Let $l \in \{0, \dots, m-2\}$. We proceed analogously to the proof of Theorem 3.19. Note that

$$R[2m-l]^G \subset R[2m-l]^H = P[m-l-1]^{H^-}$$

and therefore it follows from Proposition 3.11 that the minimal degree in x_{2m-l} of a polynomial in $R[2m-l]^G$ is greater than or equal to q^l . According to Proposition 3.6 this is the degree of

$$\psi_l(\Omega_{0,1}) = \psi_l(h_1).$$

Now, $\psi_l(h_1)$ is invariant since applying Corollary 3.5, Proposition 3.1-2 and Lemma 3.18 we would get

$$\psi_l(h_1) \in \mathbb{F}[x_1, N(x_2), \dots, N(x_l), h_1, h_2, \dots, h_l] \subset R[2m - l]^G.$$

Hence we can take $\phi_{2m-l} = \psi_l(h_1)$ for each $l \in \{0, \dots, m-1\}$.

We are now left with the task of determining for each $j \in \{1, \dots, m+1\}$, the polynomial ϕ_j . By looking at how G acts on $R[m+1]$ we can see it is acting in the same way as the group U_1 in Lemma 3.13. Hence we can choose $\phi_j = N(x_j)$ for $j \in \{1, \dots, m+1\}$. Applying Theorem 2.23 we conclude that

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_m, \dots, h_1)$$

which finishes the proof. \square

Finally, assume that the characteristic of \mathbb{F}_q is 2 and let G be the Sylow p -subgroup of $O^+(2m, q)$ given by Proposition 1.36. According to the same proposition G is generated by the element L given by (1.10) and a group G_1 with elements

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & I & 0 \\ \hline J_{m-1}(A^{-1})^T S & D & J_{m-1}(A^{-1})^T J_{m-1} \end{array} \right)$$

where A , B , I and D satisfy the conditions in Proposition 1.35 and S is such that $S + S^T = -B^T J_2 B$ and $s_{ii} = b_{1i} b_{2i}$, for $i = 1, \dots, m-1$.

Lemma 3.22 *The invariant field for G_1 is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m+1$, and the polynomials h_k , with $k = 1, \dots, m-1$, i.e.,*

$$\mathbb{F}_q(V)^{G_1} = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1}).$$

Proof: First we would like to note that in the proof of Theorem 3.21 the only time we made use of the characteristic of \mathbb{F}_q was when we applied Proposition 3.11.

If we consider the elements of G_1 with A equal to the identity matrix and B the zero matrix, then we obtain an abelian subgroup H_1 with elements

$$\left(\begin{array}{c|c|c} I_{m-1} & 0 & 0 \\ \hline 0 & I_2 & 0 \\ \hline J_{m-1}S & 0 & I_{m-1} \end{array} \right)$$

where $S \in M(m-1, q)$ is such that $S + S^T = 0$ and $s_{ii} = 0$. Hence for $C = J_{m-1}S$ we also have $c_{i, m-i} = 0$.

Now, we can use Remark 3.12 instead of Proposition 3.11 to obtain the same conclusion as in the proof of Theorem 3.21 about the minimal degrees in x_{2m-l} . The rest of the proof is similar to the one of Theorem 3.21. \square

Theorem 3.23 *Let G be the Sylow p -subgroup of $O^+(2m, q)$, with q even, given by Proposition 1.36. Then*

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m-1}), N(x_m) + N(x_{m+1}), N(x_m)N(x_{m+1}), h_1, \dots, h_{m-1}).$$

Proof: We showed in the proof of Proposition 1.36 that L normalises G_1 . Hence G_1 is a normal subgroup of G and $G/G_1 = \langle L \rangle$. From Remark 2.21 we have

$$\mathbb{F}_q(V)^G = (\mathbb{F}_q(V)^{G_1})^{\langle L \rangle}$$

and applying Lemma 3.22 we get

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1})^{\langle L \rangle}.$$

It also follows from Lemma 3.22 that

$$R := \mathbb{F}_q[x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1}]$$

is a polynomial ring. Hence $\mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1})^{\langle L \rangle}$ is the fraction field of $R^{\langle L \rangle}$.

Now, $\langle L \rangle$ is a group of order 2 and it is not hard to see that it is acting on R such that it fixes the elements $x_1, N(x_2), \dots, N(x_{m-1}), h_1, h_2, \dots, h_{m-1}$ and swaps $N(x_m)$ with $N(x_{m+1})$.

It is known that the invariant ring for the symmetric group Σ_2 acting on $\mathbb{F}_q[X, Y]$ by interchanging X with Y is generated by $X + Y$ and XY (see [25] Theorem 1.1.1). Hence

$$\begin{aligned} \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_{m-1})^{\langle L \rangle} = \\ \mathbb{F}_q(x_1, N(x_2), \dots, N(x_m), N(x_m) + N(x_{m+1}), N(x_m)N(x_{m+1}), h_1, \dots, h_{m-1}) \end{aligned}$$

and this finishes the proof. \square

3.6 The Invariant Field of a Sylow p -subgroup of $O^-(2m+2, q)$

We saw in Proposition 1.33 that $O^-(2m+2, q)$ is the group of invertible matrices that preserve the quadratic form

$$Q(v) = \sum_{i=1}^m \alpha_{2m+2-i+1} \alpha_i + \alpha_{m+1}^2 + \alpha_{m+1} \alpha_{m+2} + a \alpha_{m+2}^2,$$

where we chose a such that the polynomial $X^2 + X + a$ is irreducible in $\mathbb{F}_q[X]$ and a basis for V such that

$$v = \sum_{i=1}^m (\alpha_i u_i + \alpha_{2m+2-i+1} v_i) + \alpha_{m+1} w_1 + \alpha_{m+2} w_2.$$

Keeping in mind that now $n = 2(m+1)$, for $k \geq 1$ define

$$h_k := \Gamma_{k-1,1}$$

with $c = a$. Thus $h_1 = \sum_{i=1}^m x_{2m+2-i+1} x_i + x_{m+1}^2 + x_{m+1} x_{m+2} + a x_{m+2}^2$. We prove that h_k is invariant under the action of $O^-(2m+2, q)$ for all k .

Lemma 3.24 *For all $k \geq 1$ the polynomials h_k belong to $\mathbb{F}_q[V]^{O^-(2m+2,q)}$.*

Proof: We know from Corollary 3.3 that for $k > 1$, h_k is the q^{k-2} -th Steenrod operation of h_{k-1} and so we only need to check that h_1 is invariant. Just as in the proof of Lemma 3.20, this follows from the definition of $O^-(2m+2, q)$. \square

Just as in the previous section, we study separately the cases when q is odd and when it is even. We start with q odd. Let G be the Sylow p -subgroup of $O^-(2m+2, q)$ defined in Proposition 1.37 and $N(x_i)$ be the orbit product of x_i .

Theorem 3.25 *The invariant field $\mathbb{F}_q(V)^G$ is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m+2$, and the polynomials h_j , with $j = 1, \dots, m$, i.e.,*

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+2}), h_1, \dots, h_m).$$

Proof: If in the proof of Theorem 3.21 we replace m by $m+1$ and $\Omega_{0,1}$ by $\Gamma_{0,1}$, then we obtain a proof for this theorem. \square

Now we assume that the characteristic of \mathbb{F}_q is 2 and we denote by G the Sylow p -subgroup of $O^-(2m+2, q)$ given by Proposition 1.38. Let G_1 be the group whose elements are of the form

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline B & I & 0 \\ \hline J_m(A^{-1})^T S & D & J_m(A^{-1})^T J_m \end{array} \right)$$

with A , B , I and D satisfying the conditions in Proposition 1.37 and S is such that $S + S^T = -B^T J_2 B$ and $s_{ii} = b_{1i}^2 + b_{1i}b_{2i} + ab_{2i}^2$, for $i = 1, \dots, m$. Also, let L_1 denote the matrix

$$L_1 := \left(\begin{array}{c|c|c} I_{m-1} & 0 & 0 \\ \hline 0 & J'_2 & 0 \\ \hline 0 & 0 & I_{m-1} \end{array} \right)$$

with $J'_2 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then it follows from Proposition 1.38 that G is generated by G_1 and L_1 .

Lemma 3.26 *The invariant field for G_1 is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m+2$, and the polynomials h_k , with $k = 1, \dots, m$, i.e.,*

$$\mathbb{F}_q(V)^{G_1} = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+2}), h_1, \dots, h_m).$$

Proof: If we replace m by $m+1$ and use Theorem 3.25 instead of Theorem 3.21 in the proof of Lemma 3.22, then we get a proof for the result here stated. \square

Theorem 3.27 *Let G be the Sylow p -subgroup of $O^-(2m+2, q)$, with q even, given by Proposition 1.38. Then*

$$\begin{aligned} \mathbb{F}_q(V)^G = \\ \mathbb{F}_q(x_1, N(x_2), \dots, N(x_m), N(x_{m+1})^2 + N(x_m)N(x_{m+1}), N(x_{m+2}), h_1, \dots, h_m). \end{aligned}$$

Proof: We use similar arguments to those in the proof of Theorem 3.23. Here we can also prove that

$$\mathbb{F}_q(V)^G = (\mathbb{F}_q(V)^{G_1})^{<L_1>}.$$

Applying Lemma 3.26 we get

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+2}), h_1, \dots, h_m)^{<L_1>},$$

which is the fraction field of

$$R^{<L_1>} := \mathbb{F}_q[x_1, N(x_2), \dots, N(x_{m+2}), h_1, \dots, h_m]^{<L_1>}.$$

Now, we can easily check that $<L_1>$ is a group of order 2 acting on R by fixing $x_1, N(x_2), \dots, N(x_m), N(x_{m+2}), h_2, \dots, h_{m-1}$ and $N(x_{m+1}) \mapsto N(x_{m+1}) + N(x_m)$.

Applying Theorem 2.5 we can prove that the invariant ring of a group of order 2 acting on $\mathbb{F}_q[X, Y]$ such that it fixes X and maps Y to $Y + X$ is generated by X and $Y^2 + XY$. Hence

$$\begin{aligned} \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+2}), h_1, \dots, h_m)^{<L_1>} = \\ \mathbb{F}_q(x_1, N(x_2), \dots, N(x_m), N(x_{m+1})^2 + N(x_m)N(x_{m+1}), N(x_{m+2}), h_1, \dots, h_m) \end{aligned}$$

and the proof is complete. \square

3.7 The Invariant Field of a Sylow p -subgroup of $O(2m + 1, q)$

By Proposition 1.33, $O(2m + 1, q)$ is the group of invertible matrices that preserve the quadratic form

$$Q(v) = \sum_{i=1}^m \alpha_{2m+1-i+1} \alpha_i + \alpha_{m+1}^2,$$

where we chose a basis for V such that

$$v = \sum_{i=1}^m (\alpha_i u_i + \alpha_{2m+2-i+1} v_i) + \alpha_{m+1} w.$$

Consider the following family of polynomials: for $k \geq 1$ take

$$h_k := \Gamma_{k-1,0}.$$

In particular, $h_1 = \sum_{i=1}^m x_{n-i+1} x_i + x_{m+1}^2$. The next lemma shows that all these polynomials are invariant under the action of $O(2m + 1, q)$.

Lemma 3.28 *For all $k \geq 1$ the polynomials h_k belong to $\mathbb{F}_q[V]^{O(2m+1,q)}$.*

Proof: It follows from Corollary 3.3 that $h_k = \mathcal{P}^{q^{k-1}}(h_{k-2})$ for $k > 1$. Hence it suffices to show that h_1 is an invariant polynomial. Again as in the proof of Lemma 3.20, this follows from the definition of $O(2m + 1, q)$. \square

Now, assume that the characteristic of \mathbb{F}_q is not 2 and let G be the Sylow p -subgroup of $O(2m + 1, q)$ given by Proposition 1.39.

Theorem 3.29 *The invariant field $\mathbb{F}_q(V)^G$ is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m + 1$, and the polynomials h_k , with $k = 1, \dots, m$, i.e.,*

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_m).$$

Proof: The proof is analogous, for example, to the proofs of Theorems 3.21 or 3.17. In the same way we construct an abelian subgroup H of G which we then prove to be the subgroup H^- of Section 3.1. Therefore Proposition 3.11 tell us that q^l is a lower bound for the minimal degree in x_{2m+1-l} of an invariant polynomial in $R[2m+1-l]^G$ for every $l \in \{0, \dots, m-1\}$. Applying Propositions 3.6, Corollary 3.5, Proposition 3.1-2 and Lemma 3.28 we conclude that

$$\psi_l(\Gamma_{0,0}) = \psi_l(h_1) \in R[2m+1-l]^G$$

with degree q^l in x_{2m+1-l} .

For each $j \in \{1, \dots, m+1\}$, and using the same argument as in the proof of 3.21, we can show that the degree in x_j of $N(x_j)$ is minimal among the elements of $R[j]^G$. Now, applying Theorem 2.23 completes the proof. \square

Finally, assume that \mathbb{F}_q has characteristic 2 and let G be the Sylow p -subgroup of $O(2m+1, q)$ given by Proposition 1.40. The invariant field for G is described in the next theorem.

Theorem 3.30 *The invariant field $\mathbb{F}_q(V)^G$ is generated by the polynomials $N(x_i)$, with $i = 1, \dots, m+1$, and the polynomials h_k , with $k = 1, \dots, m$, i.e.,*

$$\mathbb{F}_q(V)^G = \mathbb{F}_q(x_1, N(x_2), \dots, N(x_{m+1}), h_1, \dots, h_m).$$

Proof: The proof is analogous to the proof of Lemma 3.22, but now we should use Theorem 3.29 instead of Theorem 3.21. \square

Chapter 4

Invariant Rings for Sylow p -subgroups of some Finite Classical Groups

In this chapter we construct the generators and 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. In contrast to this we show that this is not so in the cases above. We shall prove that these invariant rings are a complete intersection and that their generators form a *SAGBI* basis.

It is not straightforward to generalise our results to higher ranks; indeed Magma calculations show that for the Sylow p -subgroups of $Sp(6, q)$ and $O^+(6, q)$ with q odd, a similar construction does not give *SAGBI* bases. This adds more difficulty in obtaining results in the general cases and motivates further investigations.

Throughout the chapter we will always consider the graded reverse lexicographic order on $\mathbb{F}[x_1, \dots, x_n]$ with $x_1 < x_2 < \dots < x_n$, where n will be 3 or 4. Therefore if $m_1 = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ and $m_2 = x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ are two distinct monomials, $m_1 <_{\text{grevlex}} m_2$

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: first 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 $x_n^{d_n}$.

Then, we consider the algebra A generated by some of the polynomials in the list and Θ . We show that A is the invariant ring by proving that:

1. A contains a homogeneous system of parameters;
2. the fraction field of A is the invariant field;
3. A is integrally closed in its field of fractions.

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

Let G be the group defined in Proposition 1.25. Here $m = 1$ and therefore we can easily write the elements of G 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 $b\bar{b} + s + \bar{s} = 0$. Hence, G acts on the polynomial ring $\mathbb{F}_{q^2}[x_1, x_2, x_3]$ in the following way:

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

Clearly x_1 and the orbit product of x_2

$$N(x_2) = \prod_{a \in \mathbb{F}_{q^2}} (x_2 + bx_1) = x_2^{q^2} - x_1^{q^2-1}x_2$$

are invariant. From Lemma 3.16 it follows that the polynomials

$$\begin{aligned} h_1 &= \Lambda_{1,1} = x_2^{q+1} + x_3^q x_1 + x_3 x_1^q, \\ h_2 &= \Lambda_{2,1} = x_2^{q^3+1} + x_3^{q^3} x_1 + x_3 x_1^{q^3} \end{aligned}$$

are invariant under the action of G .

Lemma 4.1 *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: Applying Proposition 3.4-7 we have

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

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. \square

Lemma 4.2 *The polynomial h_2 can be written as*

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

where Θ is an invariant polynomial with leading monomial $x_3^{q^3}$.

Proof: For simplicity write $X = x_3^q + x_1^{q-1}x_3$. Hence $h_1 = x_2^{q+1} + x_1X$ and

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

Hence

$$h_2 - h_1^{q^2-q+1} = x_1 \left(x_3^{q^3} + x_1^{q^3-1} x_3 - x_2^{q^3-q} X + (x_1 X + x_2^{q+1}) \sum_{i=1}^{q-1} x_2^{(q^2+q)(q-1-i)} x_1^{qi-1} X^{qi} \right)$$

and since x_1 , h_1 and h_2 are invariant, the polynomial

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

is also invariant. \square

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 $\mathbb{F}_{q^2}[x_1, x_2, x_3]^G$.

Remark 4.3 *Let \mathbb{F} be a field and consider the graded reverse lexicographic monomial order on the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$ with $x_n > \dots > x_1$.*

1. *Suppose that $C = \{f_1, \dots, f_m\}$ is a set polynomials such that $LM(f_i) \neq LM(f_j)$ for $i \neq j$ and let $f - g = \sum_{i=1}^m f_i$. Without loss of generality we can assume that $LM(f_1) > LM(f_2) > \dots > LM(f_m)$. Therefore $\sum_{i=1}^m f_i$ is a subduction of $f - g$ over C that terminates at zero.*
2. *If in a homogeneous polynomial we have two monomials \mathbf{m}_1 and \mathbf{m}_2 such that the exponent in x_1 is non-zero, then the one with the smallest exponent, in x_1 , is the biggest monomial.*

Lemma 4.4 *The following relation*

$$h_1^{q^2} - N(x_2)^{q+1} - x_1^{q^2-1} h_1^{q^2-q+1} - x_1^{q^2} \Theta - x_1^{q(q^2-1)} h_1^q + x_1^{(q+1)(q^2-1)} h_1 = 0 \quad (4.1)$$

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 4.2, $h_2 = h_1^{q^2-q+1} + x_1\Theta$. Thus if in Lemma 4.1 we substitute h_2 by $h_1^{q^2-q+1} + x_1\Theta$, then we get the relation in the lemma. It follows from Remark 4.3 that (4.1) is a subduction of $h_1^{q^2} - N(x_2)^{q+1}$ over $\{x_1, N(x_2), h_1, \Theta\}$.

It is not hard to check that

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

So let $\phi : \mathbb{F}_{q^2}[t_1, t_2, t_3, t_4] \longrightarrow \mathbb{F}_{q^2}[x_1, x_2, x_3]$ be the \mathbb{F}_{q^2} -algebra homomorphism defined by

$$t_1 \mapsto x_1, \quad t_2 \mapsto x_2^{q^2}, \quad t_3 \mapsto x_2^{q+1}, \quad t_4 \mapsto x_3^{q^3}.$$

We will show that the kernel of ϕ is generated as an ideal by the binomial $g(t_1, t_2, t_3, t_4) = t_3^{q^2} - t_2^{q+1}$. 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 will follow from Theorem 2.35 that $\{x_1, N(x_2), h_1, \Theta\}$ is a *SAGBI* basis for A .

We keep the notation of Section 2.5. According to Corollary 2.39 the kernel of ϕ is generated by the binomials $\mathbf{T}^{\mathbf{u}^+} - \mathbf{T}^{\mathbf{u}^-}$ where $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-$ is a solution of $B\mathbf{u} = 0$. Here the matrix B is

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

and therefore the solution set for $B\mathbf{u} = 0$ is a vector space W with dimension 1. 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 2.40

$$\mathbf{T}^{\mathbf{w}^+} - \mathbf{T}^{\mathbf{w}^-} = t_3^{q^2} - t_2^{q+1}$$

generates the kernel of ϕ . This finishes the proof. \square

The next lemma will be used throughout this chapter.

Lemma 4.5 *Let $\{x_1, f_2, \dots, f_m\}$ be a homogeneous SAGBI basis for a graded subalgebra $A \subset \mathbb{F}[x_1, \dots, x_n]$ using the graded reverse lexicographic order with $x_n > \dots > x_1$. 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 $\mathbb{F}[x_1, \dots, x_n]$, we can assume without loss of generality that $g = x_1 g_1$ with $g_1 \in \mathbb{F}[x_1, \dots, x_n]$. This means that x_1 divides the leading monomial of g and therefore it divides all the other monomials. Hence, at every stage in the subduction of g over $\{x_1, f_2, \dots, f_m\}$, x_1 will be a factor. Since x_1 does not divide $LM(f_i)$ for all $i > 1$ and $\{x_1, f_2, \dots, f_m\}$ is a SAGBI basis for A , we can write g as $x_1 g'$ with $g' \in A$. Thus $g \in A$ and this completes the proof. \square

Theorem 4.6 *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 (4.1).

Proof: Applying Lemma 2.14 we conclude that $\{x_1, N(x_2), h_1, \Theta\}$ contains a homogeneous system of parameters for $\mathbb{F}_{q^2}[x_1, x_2, x_3]^G$. Hence, $\mathbb{F}_{q^2}[x_1, x_2, x_3]$ is integral over A .

It follows from Theorem 3.17 that

$$\mathbb{F}_{q^2}(x_1, x_2, x_3)^G = \mathbb{F}_{q^2}(x_1, N(x_2), h_1).$$

Since

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

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. We start by showing that the localisation $A[x_1^{-1}]$ is a Unique Factorisation Domain. Since x_1 is invertible in $A[x_1^{-1}]$, from (4.1) 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 4.4 and 4.5 it follows that the ideal of A generated by x_1 is a prime. Hence applying Lemma 2.24 we conclude that A is integrally closed and this finishes the proof. \square

Remark 4.7 *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 4.8 *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 (4.1) that $P(X_1, X_2, X_3, X_4)$ belongs to the kernel of Φ . Note that $P(X_1, X_2, X_3, X_4)$ is linear in X_4 and X_1 is the only irreducible dividing the coefficient of X_4 . Since X_1 does not divide all the other terms in $P(X_1, X_2, X_3, X_4)$ 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.

The Krull dimension of A is 3 by Corollary 2.17. 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 $P(X_1, X_2, X_3, X_4)$. Thus A is a complete intersection ring by definition 2.19. \square

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

Consider the group G given by Proposition 1.24, which is a Sylow p -subgroup of $GU(4, q^2)$. It is not hard to see that its elements are

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

where $b_1, b_2, c, s \in \mathbb{F}_{q^2}$ such that $c + \bar{c} = 0$ and $s + \bar{s} = -b_1 \bar{b}_2 - b_2 \bar{b}_1$. Hence, the action of G on $\mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]$ is defined by

- $x_1 \mapsto x_1, x_2 \mapsto x_2 + b_1 x_1, x_3 \mapsto x_3 + c x_2 + b_2 x_1$ and
- $x_4 \mapsto x_4 - \bar{b}_1 x_3 - (\bar{b}_1 \bar{c} + \bar{b}_2) x_2 + s x_1$.

It follows from Lemma 2.28 that 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. Applying Lemma 3.14 we get that the polynomials

- $h_1 = \Lambda_{1,0} = x_3^q x_2 + x_3 x_2^q + x_4^q x_1 + x_4 x_1^q$;
- $h_2 = \Lambda_{2,0} = x_3^{q^3} x_2 + x_3 x_2^{q^3} + x_4^{q^3} x_1 + x_4 x_1^{q^3}$;
- $h_3 = \Lambda_{3,0} = x_3^{q^5} x_2 + x_3 x_2^{q^5} + x_4^{q^5} x_1 + x_4 x_1^{q^5}$;

are also invariant under the action of G .

Lemma 4.9 *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

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

Proof: This is a consequence of Proposition 3.4 and the definition of ψ_1 .

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 write $X = x_3^{q^2} - x_1^{q^2-1}x_3$, then $\psi_1(x_3) = X$. Therefore

$$\begin{aligned} N(x_2)N(x_3) &= N(x_2)(X^q + N(x_2)^{q-1}X) = N(x_2)X^q + N(x_2)^qX \\ &= \psi_1(x_3)^q\psi_1(x_2) + \psi_1(x_3)\psi_1(x_2)^q = \psi_1(h_1) \end{aligned}$$

and according to Proposition 3.4-7

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

Finally, we have

$$\begin{aligned}
N(x_2)N(x_3)^{q^2} &= N(x_2)(X^{q^3} + N(x_2)^{q^3-q^2}X^{q^2}) = N(x_2)X^{q^3} + N(x_2)^{q^3-q^2+1}X^{q^2}; \\
N(x_2)^{q^3-q^2+1}N(x_3)^q &= N(x_2)^{q^3-q^2+1}X^{q^2} + N(x_2)^{q^3-q+1}X^q; \\
N(x_2)^{q^3-q+1}N(x_3) &= N(x_2)^{q^3-q+1}X^q + N(x_2)^{q^3}X;
\end{aligned}$$

and therefore

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

From Proposition 3.4-8 we get

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

This completes the proof. \square

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

$$\begin{aligned}
f_1 := \overline{N(x_2)} &= x_2^{q^2}, \quad f_2 := \overline{N(x_3)} = x_3^{q^3} + x_2^{q^3-q^2}x_3^{q^2}, \quad f_3 := \overline{h_1} = x_3^q x_2 + x_3 x_2^q \\
f_4 &:= \overline{h_2} = x_3^{q^3} x_2 + x_3 x_2^{q^3} \quad \text{and} \quad f_5 := \overline{h_3} = x_3^{q^5} x_2 + x_3 x_2^{q^5}
\end{aligned}$$

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

Lemma 4.10 *The set of polynomials $\{f_1, f_2, f_3, f_4\}$ 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 4.4 and Example 2.42 to show that C is a SAGBI basis for A . Here the leading monomials are

$$LM(f_1) = x_2^{q^2}, \quad LM(f_2) = x_3^{q^3}, \quad LM(f_3) = x_3^q x_2, \quad \text{and} \quad LM(f_4) = x_3^{q^3} x_2$$

Thus the \mathbb{F}_{q^2} -algebra homomorphism $\phi : \mathbb{F}_{q^2}[t_1, t_2, t_3, t_4] \longrightarrow \mathbb{F}_{q^2}[x_2, x_3]$ is defined by

$$t_1 \mapsto x_2^{q^2}, \quad t_2 \mapsto x_3^{q^3}, \quad t_3 \mapsto x_3^q x_2, \quad t_4 \mapsto x_3^{q^3} x_2$$

and the corresponding matrix B 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 we can easily check that

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

form a basis for W . As in Example 2.42 we can show that **Hypothesis A** holds for the basis $\{\mathbf{w}_1, \mathbf{w}_2\}$. Hence

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

generate the $\ker \phi$ by Proposition 2.41.

According to Theorem 2.35 we should check if

$$g_1(f_1, f_2, f_3, f_4) = f_3^{q^2} - f_1 f_2 \text{ and } g_2(f_1, f_2, f_3, f_4) = f_4^{q^2} - f_1 f_2^{q^2}$$

have a subduction over C that terminates at a constant. It follows from Lemma 4.9 that

$$f_3^{q^2} - f_1 f_2 = 0 \tag{4.2}$$

$$f_4^{q^2} - f_1 f_2^{q^2} - f_1^{q^3 - q^2 + 1} f_2^q + f_1^{q^3 - q + 1} f_2 = 0. \tag{4.3}$$

Applying Remark 4.3 we conclude that (4.2) and (4.3) 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, to prove that the polynomial f_5 has a subduction over $\{f_1, f_2, f_3, f_4\}$ terminating at zero, it is enough to show that $f_5 \in A$. 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

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

and

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

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 (4.2) and (4.3) we conclude that $f_4^{q^2}$ is divisible by $f_3^{q^2}$. Hence $f_5 \in A$ and this finishes the proof. \square

Let $P(X_1, X_2, X_3, X_4)$ be the polynomial obtained in the subduction of f_5 over $\{f_1, f_2, f_3, f_4\}$, i.e., $f_5 = P(f_1, f_2, f_3, f_4)$.

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

$$\Theta := x_4^{q^5} + x_1^{q^5-1}x_4 + \dots$$

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 4.11 *The following relations*

$$h_1^{q^2} - N(x_2)N(x_3) - x_1^{q^2-1}h_2 - x_1^{q(q^2-1)}h_1^q + x_1^{(q+1)(q^2-1)}h_1 = 0 \quad (4.4)$$

and

$$\begin{aligned} & h_2^{q^2} - N(x_2)N(x_3)^{q^2} + N(x_2)^{q^3-q^2+1}N(x_3)^q - N(x_2)^{q^3-q+1}N(x_3) \\ & - x_1^{q^2-1}P(N(x_2), N(x_3), h_1, h_2) - x_1^{q^2}\Theta \\ & - x_1^{q^3(q^2-1)}h_1^{q^2} + x_1^{(q^3+1)(q^2-1)}h_2 = 0 \end{aligned} \quad (4.5)$$

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 $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$. Applying Remark 4.3 we conclude that (4.4) and (4.5) 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 \mathbb{F}_{q^2} -algebra homomorphism $\phi : \mathbb{F}_{q^2}[t_1, t_2, t_3, t_4, t_5, t_6] \longrightarrow \mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]$ is then defined by

$$t_1 \mapsto x_1, t_2 \mapsto x_2^{q^2}, t_3 \mapsto x_3^{q^3}, t_4 \mapsto x_3^q x_2, t_5 \mapsto x_3^{q^3} x_2, t_6 \mapsto x_4^{q^5}$$

and the matrix B 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 4.10, we can show that the vectors

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

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

$$\begin{aligned}g_1(t_1, t_2, t_3, t_4, t_5, t_6) &= t_4^{q^2} - t_2 t_3, \\ g_2(t_1, t_2, t_3, t_4, t_5, t_6) &= t_5^{q^2} - t_2 t_3^{q^2}\end{aligned}$$

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

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

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. \square

Theorem 4.12 *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.,*

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

Furthermore, the generators satisfy the relations (4.4) and (4.5).

Proof: Since $\{x_1, N(x_2), N(x_3), \Theta\}$ is a homogeneous system of parameters for $\mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]^G$ by Lemma 2.14, the polynomial ring $\mathbb{F}_{q^2}[x_1, x_2, x_3, x_4]$ is integral over A .

According to Theorem 3.15 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

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

we conclude that $\text{Quot}(A)$ is equal to $\mathbb{F}_{q^2}(x_1, x_2, x_3, x_4)^G$.

Finally, we show that A is integrally closed. Consider the ring $A[x_1^{-1}]$. Since x_1 is invertible in $A[x_1^{-1}]$, it follows from (4.4) and (4.5) 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 4.11 and 4.5 we conclude that the ideal of A generated by x_1 is prime. Hence A is integrally closed by Lemma 2.24. \square

Remark 4.13 *We would like to note that $C := \{x_1, N(x_2), h_1, h_2, N(x_4)\}$ 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 polynomial 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 4.14 *The kernel of Φ is generated by the polynomials*

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

and

$$\begin{aligned} P_2(X_1, X_2, X_3, X_4, Z_1, Z_2) &:= Z_2^{q^2} - X_2 X_3^{q^2} + X_2^{q^3-q^2+1} X_3^q - X_2^{q^3-q+1} X_3 \\ &- X_1^{q^2-1} P(X_2, X_3, Z_1, Z_2) - X_1^{q^2} X_4 - X_1^{q^3(q^2-1)} Z_1^{q^2} + X_1^{(q^3+1)(q^2-1)} Z_2 \end{aligned}$$

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 $R := \mathbb{F}_{q^2}[X_1, X_2, X_3, X_4, Z_1, Z_2]$. Applying Corollary 2.17 we conclude that the Krull dimension of A is 4. Since

$$R/\ker \Phi \simeq A,$$

the kernel of Φ is a prime ideal of height 2.

From (4.4) and (4.5) 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

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

respectively. Hence \overline{P}_1 is not a zero-divisor in $R/(X_1)$. Also since \overline{P}_1 is linear in \overline{X}_3 and \overline{X}_2 does not divide $\overline{Z}_1^{q^2}$ we conclude that \overline{P}_1 is irreducible in $R/(X_1)$. Therefore $R/(X_1, P_1) = (R/(X_1))/(\overline{P}_1)$ is an integral domain. It is easy to check that \overline{P}_2 is not a zero divisor in $(R/(X_1))/(\overline{P}_1)$. 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. Hence $R/(P_1, P_2)[\bar{X}_1^{-1}]$ is the localisation of a polynomial ring, thus a domain. Therefore (P_1, P_2) is a prime ideal.

Finally, A is a complete intersection by Definition 2.19. \square

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

Consider the group G given by Proposition 1.27, which is a Sylow p -subgroup of $Sp(4, q)$. It is not hard to see that its elements are

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

with $b_1, b_2, c, s \in \mathbb{F}_q$. Therefore, G acts on $\mathbb{F}_q[x_1, x_2, x_3, x_4]$ by

- $x_1 \mapsto x_1, x_2 \mapsto x_2 + b_1x_1, x_3 \mapsto x_3 + cx_2 + b_2x_1$ and
- $x_4 \mapsto x_4 - b_1x_3 + (-b_1c + b_2)x_2 + sx_1$.

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. By Lemma 3.18 the polynomials

- $h_1 = \Omega_{1,-1} = x_3^q x_2 - x_3 x_2^q + x_4^q x_1 - x_4 x_1^q;$
- $h_2 = \Omega_{2,-1} = x_3^{q^2} x_2 - x_3 x_2^{q^2} + x_4^{q^2} x_1 - x_4 x_1^{q^2};$

- $h_3 = \Omega_{3,-1} = x_3^{q^3}x_2 - x_3x_2^{q^3} + x_4^{q^3}x_1 - x_4x_1^{q^3}$

are invariant.

Lemma 4.15 *The polynomials x_1 , $N(x_2)$, $N(x_3)$, h_1 , h_2 and h_3 satisfy*

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

and

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

Proof: Similar calculations to the ones in the proof of Lemma 4.9.

Here we have $\psi_1(x_2) = x_2^q - x_1^{q-1}x_2 = N(x_2)$ and $X := \psi_1(x_3) = x_3^q - x_1^{q-1}x_3$. Thus

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

and we just need to apply Proposition 3.4-3 to determine $\psi_1(h_1)$.

Now, we have

$$\begin{aligned} N(x_2)N(x_3)^q &= N(x_2)(X^{q^2} - N(x_2)^{q^2-q}X^q) = N(x_2)X^{q^2} - N(x_2)^{q^2-q+1}X^q; \\ N(x_2)^{q^2-q+1}N(x_3) &= N(x_2)^{q^3-q+1}X^q - N(x_2)^{q^2}X. \end{aligned}$$

Therefore

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

and the result follows again from Proposition 3.4-3. This completes the proof. \square

Just as in the previous section, if we consider the modulo x_1 reductions of the polynomials x_1 , $N(x_2)$, $N(x_3)$, h_1 , h_2 and h_3 we obtain polynomials

$$\begin{aligned} f_1 := \overline{N(x_2)} &= x_2^q, & f_2 := \overline{N(x_3)} &= x_3^{q^2} - x_2^{q^2-q}x_3^q, & f_3 := \overline{h_1} &= x_3^qx_2 - x_3x_2^q \\ f_4 &:= \overline{h_2} = x_3^{q^2}x_2 - x_3x_2^{q^2} & \text{and} & & f_5 := \overline{h_3} &= x_3^{q^3}x_2 - x_3x_2^{q^3} \end{aligned}$$

which we can think as being elements in $\mathbb{F}_q[x_2, x_3]$. Also, we consider the graded reverse lexicographic order on $\mathbb{F}_q[x_2, x_3]$ with $x_2 < x_3$.

Lemma 4.16 *The set of polynomials $\{f_1, f_2, f_3, f_4\}$ is a SAGBI basis for $\mathbb{F}_q[f_1, f_2, f_3, f_4]$ and the polynomial f_5 has a subduction over $\{f_1, f_2, f_3, f_4\}$ that terminates at zero.*

Proof: The proof is analogous to the proof of Lemma 4.10. Let A denote the algebra $\mathbb{F}_q[f_1, f_2, f_3, f_4]$ and $C = \{f_1, f_2, f_3, f_4\}$.

Here the \mathbb{F}_q -algebra homomorphism $\phi : \mathbb{F}_q[t_1, t_2, t_3, t_4] \longrightarrow \mathbb{F}_q[x_1, x_2]$ is defined by

$$t_1 \mapsto x_2^q, \quad t_2 \mapsto x_3^{q^2}, \quad t_3 \mapsto x_3^q x_2, \quad t_4 \mapsto x_3^{q^2} x_2$$

and the corresponding matrix B is

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

The set of solutions for $B\mathbf{u} = 0$ is a vector space W with dimension 2, for which the vectors

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

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

form a basis. As in Example 2.42 we can show that **Hypothesis A** is satisfied by $\{\mathbf{w}_1, \mathbf{w}_2\}$. Hence

$$g_1(t_1, t_2, t_3, t_4) = t_3^q - t_1 t_2 \quad g_2(t_1, t_2, t_3, t_4) = t_4^q - t_1 t_2^q$$

generate $\ker \phi$ by Proposition 2.41. Now, it follows from Lemma 4.15 that

$$f_3^q - f_1 f_2 = 0 \tag{4.6}$$

$$f_4^q - f_1 f_2^q - f_1^{q^2-q+1} f_2 = 0. \tag{4.7}$$

Applying Remark 4.3 we obtain that (4.6) and (4.7) 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 by Theorem 2.35.

Finally, we show that $f_5 \in A$. It is easy to check that

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

Therefore

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

and we obtain

$$f_3^q f_5 = f_4^{q+1} - f_3^{q^2+1}.$$

From (4.6) and (4.7) we conclude that f_4^q is divisible by f_3^q . Hence $f_5 \in A$ and this finishes the proof. \square

Let $P(X_1, X_2, X_3, X_4)$ denote the polynomial obtained in the subduction of f_5 over $\{f_1, f_2, f_3, f_4\}$, i.e, $f_5 = P(f_1, f_2, f_3, f_4)$. Since $h_1 = f_3 + x_1(x_4^q - x_1^{q-1}x_4)$, $h_2 = f_4 + x_1(x_4^{q^2} - x_1^{q^2-1}x_4)$ and x_4 does not appear in $N(x_2)$ and $N(x_3)$, we conclude that the monomial $x_1x_4^{q^3}$ will not occur in $P(N(x_2), N(x_3), h_1, h_2)$. Hence we obtain

$$h_3 = f_5 + x_1(x_4^{q^3} - x_1^{q^3-1}x_4) = P(N(x_2), N(x_3), h_1, h_2) + x_1\Theta,$$

where

$$\Theta := x_4^{q^3} - x_1^{q^3-1}x_4 + \dots$$

is an invariant polynomial under the action of G .

Now, let A be the \mathbb{F}_q -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 $Sp(4, q)$.

Lemma 4.17 *The following relations*

$$h_1^q - N(x_2)N(x_3) - x_1^{q-1}h_2 + x_1^{q(q-1)}h_1 = 0 \tag{4.8}$$

and

$$\begin{aligned} & h_2^q - N(x_2)N(x_3)^q - N(x_2)^{q^2-q+1}N(x_3) - x_1^{q-1}P(N(x_2), N(x_3), h_1, h_2) - x_1^q\Theta \\ & - x_1^{q(q-1)}h_1^q + x_1^{(q^2+1)(q-1)}h_2 = 0 \end{aligned} \quad (4.9)$$

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

Proof: The proof is analogous to the one of Lemma 4.11. Here we get that

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

is a subduction of $x_1^{q-1}h_3$ over $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$. Applying Remark 4.3 to (4.6) and (4.7) we finish the first part of the proof.

Now the \mathbb{F}_q -algebra homomorphism $\phi : \mathbb{F}_q[t_1, t_2, t_3, t_4, t_5, t_6] \longrightarrow \mathbb{F}_q[x_1, x_2, x_3, x_4]$ is defined by

$$t_1 \mapsto x_1, t_2 \mapsto x_2^q, t_3 \mapsto x_3^{q^2}, t_4 \mapsto x_3^q x_2, t_5 \mapsto x_3^{q^2} x_2, t_6 \mapsto x_4^{q^3}.$$

Then the matrix B is

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

Analogously to what was done in the proof Lemma 4.10 we can show that the vectors

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

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

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

$$g_1(t_1, t_2, t_3, t_4, t_5, t_6) = t_4^q - t_2 t_3,$$

$$g_2(t_1, t_2, t_3, t_4, t_5, t_6) = t_5^q - t_2 t_3^q$$

generate $\ker \phi$. Since

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

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

Theorem 4.18 *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.,*

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

Furthermore, the generators satisfy the relations (4.8) and (4.9).

Proof: The proof is analogous to the one of Theorem 4.12. \square

Remark 4.19 *The argument in Remark 4.13 can also be used here to show that $\{x_1, N(x_2), h_1, h_2, N(x_4)\}$ is also a generating set for the invariant ring $\mathbb{F}_q[x_1, x_2, x_3, x_4]^G$, where $N(x_4)$ is the orbit product of x_4 .*

Finally, we will show that the invariant ring for G is a complete intersection. We consider the polynomial ring $\mathbb{F}_q[X_1, X_2, X_3, X_4, Z_1, Z_2]$ and the homomorphism

$$\Phi : \mathbb{F}_q[X_1, X_2, X_3, X_4, Z_1, Z_2] \longrightarrow A$$

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 4.20 *The kernel of Φ is generated by the polynomials*

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

and

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

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 ring.

Proof: The proof is analogous to the one of Lemma 4.14. \square

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

Consider the group G given by Proposition 1.27, which is a Sylow p -subgroup of $O^+(4, q)$ for q odd. It is not hard to see that its elements are

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

with $b_1, b_2 \in \mathbb{F}_q$. Therefore, G acts on $\mathbb{F}_q[x_1, x_2, x_3, x_4]$ by

- $x_1 \mapsto x_1, x_2 \mapsto x_2 + b_1 x_1, x_3 \mapsto x_3 + b_2 x_1$ and
- $x_4 \mapsto x_4 - b_1 x_3 - b_2 x_2 - b_1 b_2 x_1$.

It is not hard to see that the orbit products of x_2 and x_3 are

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

respectively. By Lemma 3.20 the polynomials

- $h_1 = \Omega_{0,1} = x_3x_2 + x_4x_1$;
- $h_2 = \Omega_{1,1} = x_3^qx_2 + x_3x_2^q + x_4^qx_1 + x_4x_1^q$;
- $h_3 = \Omega_{2,1} = x_3^{q^2}x_2 + x_3x_2^{q^2} + x_4^{q^2}x_1 + x_4x_1^{q^2}$

are also invariant.

Lemma 4.21 *The polynomials x_1 , $N(x_2)$, $N(x_3)$, h_1 , h_2 and h_3 satisfy*

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

and

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

Proof: We can easily see that $\psi_1(x_2) = N(x_2)$ and $\psi_1(x_3) = N(x_3)$. Hence we get $\psi_1(h_1) = N(x_2)N(x_3)$ and $\psi_1(h_2) = N(x_2)N(x_3)^q + N(x_2)^qN(x_3)$. Now applying Proposition 3.4-1 and 2 we finish the proof. \square

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

$$\begin{aligned} f_1 := \overline{N(x_2)} &= x_2^q, & f_2 := \overline{N(x_3)} &= x_3^q, & f_3 := \overline{h_1} &= x_3x_2, \\ f_4 &:= \overline{h_2} = x_3^qx_2 + x_3x_2^q & \text{and} & & f_5 := \overline{h_3} &= x_3^{q^2}x_2 + x_3x_2^q \end{aligned}$$

belonging to $\mathbb{F}_q[x_2, x_3]$. Once more we consider the graded reverse lexicographic order on $\mathbb{F}_q[x_2, x_3]$ with $x_2 < x_3$.

Lemma 4.22 *The set of polynomials $\{f_1, f_2, f_3, f_4\}$ is a SAGBI basis for $\mathbb{F}_q[f_1, f_2, f_3, f_4]$ and the polynomial f_5 has a subduction over $\{f_1, f_2, f_3, f_4\}$ that terminates at zero.*

Proof: The proof is analogous to the proof of Lemma 4.10. Let A denote the algebra $\mathbb{F}_q[f_1, f_2, f_3, f_4]$ and $C = \{f_1, f_2, f_3, f_4\}$.

Now the \mathbb{F}_q -algebra homomorphism $\phi : \mathbb{F}_q[t_1, t_2, t_3, t_4] \longrightarrow \mathbb{F}_q[x_1, x_2]$ is defined by

$$t_1 \mapsto x_2^q, \quad t_2 \mapsto x_3^q, \quad t_3 \mapsto x_3 x_2, \quad t_4 \mapsto x_3^q x_2.$$

The matrix B is

$$\begin{pmatrix} q & 0 & 1 & 1 \\ 0 & q & 1 & q \end{pmatrix}$$

and the solution set for $B\mathbf{u} = 0$ is a 2-dimensional vector space W for which the vectors

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

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

form a basis. Just as we did in Example 2.42, we can show that **Hypothesis A** is satisfied by $\{\mathbf{w}_1, \mathbf{w}_2\}$. Hence

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

generate $\ker \phi$ by Proposition 2.41. It follows from Lemma 4.21 that

$$f_3^q - f_1 f_2 = 0 \tag{4.10}$$

$$f_4^q - f_1 f_2^q - f_1^q f_2 = 0. \tag{4.11}$$

Applying Remark 4.3 we conclude that (4.10) and (4.11) 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 by Theorem 2.35.

Now we show that $f_5 \in A$. A straightforward calculation shows that

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

Thus if we take

$$f := 4f_3^{q+1} - f_4^2 = \begin{vmatrix} x_3 & x_2 \\ x_3^q & x_2^q \end{vmatrix} \begin{vmatrix} x_2 & x_2^q \\ x_3 & x_3^q \end{vmatrix} = - \begin{vmatrix} x_2 & x_2^q \\ x_3 & x_3^q \end{vmatrix}^2$$

and

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

we obtain $0 = f^{\frac{q+1}{2}} + (-1)^{\frac{q+1}{2}} g$ and therefore

$$2(-1)^{\frac{q+1}{2}} f_3^q f_5 = (-1)^{\frac{q+1}{2}} f_4^{q+1} - (4f_3^{q+1} - f_4^2)^{\frac{q+1}{2}}.$$

From (4.10) and (4.11) we conclude that f_4^q is divisible by f_3^q . Hence $f_5 \in A$ and this finishes the proof. \square

We denote by $P(X_1, X_2, X_3, X_4)$ the polynomial obtained from the subduction of f_5 over $\{f_1, f_2, f_3, f_4\}$, i.e, $f_5 = P(f_1, f_2, f_3, f_4)$. Since $h_1 = f_3 + x_1 x_4$, $h_2 = f_4 + x_1(x_4^q + x_1^{q-1} x_4)$ and x_4 does not appear in the polynomials $N(x_2)$ and $N(x_3)$, we conclude that the monomial $x_1 x_4^{q^2}$ will not occur in $P(N(x_2), N(x_3), h_1, h_2)$. Therefore we obtain

$$h_3 = f_5 + x_1(x_4^{q^2} + x_1^{q^2-1} x_4) = P(N(x_2), N(x_3), h_1, h_2) + x_1 \Theta,$$

where

$$\Theta := x_4^{q^2} + x_1^{q^2-1} x_4 + \dots$$

is an invariant polynomial under the action of G .

Let A be the \mathbb{F}_q -algebra generated by the polynomials x_1 , $N(x_2)$, $N(x_3)$, h_1 , h_2 and Θ . We will prove that A is the invariant ring for the Sylow p -subgroup of $O^+(4, q)$ with q odd.

Lemma 4.23 *The following relations*

$$h_1^q - N(x_2)N(x_3) - x_1^{q-1}h_2 + x_1^{2q-2}h_1 = 0 \tag{4.12}$$

and

$$\begin{aligned} & h_2^q - N(x_2)N(x_3)^q - N(x_2)^q N(x_3) - x_1^{q-1}P(N(x_2), N(x_3), h_1, h_2) - x_1^q \Theta \\ & - 2x_1^{q(q-1)}h_1^q + x_1^{(q+1)(q-1)}h_2 = 0 \end{aligned} \quad (4.13)$$

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

Proof: The proof is analogous to the ones of Lemmas 4.11 and 4.17. Here the \mathbb{F}_q -algebra homomorphism $\phi : \mathbb{F}_q[t_1, t_2, t_3, t_4, t_5, t_6] \longrightarrow \mathbb{F}_q[x_1, x_2, x_3x_4]$ is defined by

$$t_1 \mapsto x_1, t_2 \mapsto x_2^q, t_3 \mapsto x_3^q, t_4 \mapsto x_3x_2, t_5 \mapsto x_3^qx_2, t_6 \mapsto x_4^{q^2}.$$

Then we can prove that

$$\begin{aligned} \mathbf{w}_1 &= (0, -1, -1, q, 0, 0) = (0, 0, 0, q, 0, 0) - (0, 1, 1, 0, 0, 0) \\ \mathbf{w}_2 &= (0, -1, -q, 0, q, 0) = (0, 0, 0, 0, q, 0) - (0, 1, q, 0, 0, 0) \end{aligned}$$

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

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

Since

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

have a subduction over $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$ that terminates at zero, we conclude that $\{x_1, N(x_2), N(x_3), h_1, h_2, \Theta\}$ is a *SAGBI* basis for A . \square

Theorem 4.24 *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.,*

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

Furthermore, the generators satisfy the relations (4.12) and (4.13).

Proof: The proof is analogous to the one of Theorem 4.12. \square

Remark 4.25 *Just as in the previous sections, we can show that $\{x_1, N(x_2), h_1, h_2, N(x_4)\}$ is a also generating set for the invariant ring $\mathbb{F}_q[x_1, x_2, x_3, x_4]^G$, where $N(x_4)$ is the orbit product of x_4 . The same reasoning as in Remark 4.13 suffices.*

We can also show that the invariant ring for G is a complete intersection. Let us consider the polynomial ring $\mathbb{F}_q[X_1, X_2, X_3, X_4, Z_1, Z_2]$ and the homomorphism

$$\Phi : \mathbb{F}_q[X_1, X_2, X_3, X_4, Z_1, Z_2] \longrightarrow A$$

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 4.26 *The kernel of Φ is generated by the polynomials*

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

and

$$\begin{aligned} P_2(X_1, X_2, X_3, X_4, Z_1, Z_2) &:= Z_2^q - X_2X_3^q - X_2^qX_3 - X_1^{q-1}P(X_2, X_3, Z_1, Z_2) \\ &- X_1^qX_4 - 2X_1^{q(q-1)}Z_1^q + X_1^{(q+1)(q-1)}Z_2 \end{aligned}$$

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 ring.

Proof: The proof is analogous to the one of Lemma 4.14. \square

Bibliography

- [1] M. Aschbacher, *Finite group theory*, Cambridge University Press, Cambridge, 1986.
- [2] M.F. Atiyah and I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1969.
- [3] David Benson, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Notes Series, vol. 190, Cambridge University Press, Cambridge, 1993.
- [4] H.E.A. Campbell and J. Chuai, *Invariant fields and localized invariant rings of p -groups*, The Quarterly Journal of Mathematics **58** (2007), 151–157.
- [5] Ming chang Kang, *Fixed fields of triangular matrix groups*, Journal of Algebra **302** (2006), 845–847.
- [6] C.W.Wilkerson, *A primer on the dickson invariants*, Contemporary Mathematics **19** (1983), 421–434.
- [7] Harm Derksen and Gregor Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 130, Springer-Verlag, 2002.
- [8] L.E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. A.M.S. **12** (1911), 75–98.

- [9] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York, 1995.
- [10] P. Fleischmann G. Kemper and C. Woodcock, *Homomorphisms, localizations, and a new algorithm to construct invariant rings of finite groups*, J. ALgebra **309** (2007), 497–517.
- [11] P. Gordon, *Beweis, dass jede covariante und invariante einer binären form eine ganze funktion mit numerischen coefficienten einer endlichen anzahl solcher formen ist*, J. Reine Angew. Math. **69** (1868), 323–354.
- [12] Larry C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, Rhode Island, 2001.
- [13] William J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. **102** (1975), 67–83.
- [14] David Hilbert, *Über die theorie der algebraischen formen*, Math. Ann. **36** (1890), 473–534.
- [15] D. Kapur and K. Madlener, *A completion procedure for computing a canonical basis for a k -subalgebra*, Proceedings of Computers and Mathematics (S. Watt E. Kaltofen, ed.), MIT, Cambridge, Mass., 1989, pp. 1–11.
- [16] Gregor Kemper, *Calculating invariants rings of finite groups over arbitrary fields*, J. Symbolic Comput. **21** (1996), 351–366.
- [17] ———, *A constructive approach to noether’s problem*, Manuscripta Math. **90** (1996), 343–363.
- [18] Gregor Kemper and Gunter Malle, *The finite irreducible linear groups with a polynomial ring of invariants*, Transformation Groups **2** (1997), 57–89.

- [19] T. Miyata, *Invariants of certain groups i*, Nagoya Math. J. **41** (1971), 69–73.
- [20] Masayoshi Nagata, *On the 14th problem of hilbert*, Am. J. Math. **81** (1959), 766–772.
- [21] ———, *Invariants of a group in an affine ring*, J. Math. Kyoto University **3** (1963/1964), 369–377.
- [22] H. Nakajima, *Invariants of finite groups generated by pseudoreflections*, Tsukuba J. Math. **3** (1979), 109–122.
- [23] Emmy Noether, *Der endlichkeitssatz der invariante endlicher linearer gruppen der charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28–25.
- [24] Lorenzo Robbiano and Moss Sweedler, *Subalgebras bases*, Lecture Notes in Mathematics, vol. 1430, Springer-Verlag, Berlin, 1990, pp. 61–87.
- [25] Larry Smith, *Polynomial invariants of finite groups*, A. K. Peters, Wellesley, Mass., 1995.
- [26] Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, 1996.
- [27] D.E. Taylor, *The geometry of the classical groups*, Heldermann Verlag, Berlin, 1992.
- [28] Herman Weyl, *Theorie der darstellung kontinuierlicher halbeinfacher gruppen durch lineare transformationen ii, iii, iv*, Math. Z. **24** (1926), 328–376, 377–395, 789–791.