Homological Properties of Invariant Rings of Finite Groups

by

Fawad Hussain

A thesis submitted to the
College of Science and Engineering
at the University of Glasgow
for the degree of
Doctor of Philosophy

November 2011

Abstract

Let V be a non-zero finite dimensional vector space over the finite field F_q. We take the left action of $G \leq GL(V)$ on V and this induces a right action of G on the dual of V which can be extended to the symmetric algebra $F_q[V]$ by ring automorphisms. In this thesis we find the explicit generators and relations among these generators for the ring of invariants $F_q[V]^G$. The main body of the research is in chapters 4, 5 and 6. In chapter 4, we consider three subgroups of the general linear group which preserve singular alternating, singular hermitian and singular quadratic forms respectively, and find rings of invariants for these groups. We then go on to consider, in chapter 5, a subgroup of the symplectic group. We take two special cases for this subgroup. In the first case we find the ring of invariants for this group. In the second case we progress to the ring of invariants for this group but the problem is still open. Finally, in chapter 6, we consider the orthogonal groups in even characteristic. We generalize some of the results of [24]. This generalization is important because it will help to calculate the rings of invariants of the orthogonal groups over any finite field of even characteristic.

Acknowledgements

I am very thankful to God, the almighty, for granting me the requisite energy and capability to complete the task which was assigned to me.

I am very grateful to my supervisor Professor Peter Kropholler and I would like to thank him for his support, advice and encouragement during this research.

I would also like to thank my Second supervisor Professor Kenny Brown for his help and guidance when i needed it in my research.

I would like to acknowledge my officemates: Joe, Steven, Ewan, Beibei and Yujue for their continued help throughout the last three years.

I would also like to acknowledge my flat mates: Sardar, Javed, Sajjad and Jehan for supporting and facilitating me during the past three years.

I would like to thank my family members, particularly my parents for always remembering me in their prayers and extending all possible help.

Finally, I would like to thank for their financial support for this research provided by Higher Education Commission and Hazara University Pakistan.

Statement

This thesis is submitted in accordance with the regulations for the degree of Doctor of Philosophy in the University of Glasgow.

No part of this thesis has previously been submitted by me for a degree at this or any other university.

Contents

Chapter 0

Introduction

Let V be a finite dimensional vector space over the finite field F_q with basis $e_1, \ldots, e_n$. Suppose $x_1, \ldots, x_n$ is the dual basis of the dual vector space V^*. Let $G \leq GL(V)$ and consider the polynomial ring in the n indeterminates $F_q[x_1, \ldots, x_n]$. Invariant theory over finite fields is a branch of abstract algebra. The theory deals with those elements of $F_q[x_1, \ldots, x_n]$ which do not change under the action of the group G. These elements form a ring structure which is called the ring of invariants of the group G.

This thesis is concerned with the invariant theory of finite groups. For a long time there has been interest in finding the ring of invariants of the group $G \leq GL(V)$. The rings of invariants of the general linear and the special linear groups were computed early in the 20th century by Dickson in [16]. These were found to be a graded polynomial algebras in both cases. For a modern treatment see Wilkerson [43]. Wilkerson also deals with the ring of invariants of the whole general linear group. There is another important paper by Carlisle and Kropholler [9]. These authors found explicit generators for the rational invariants of orthogonal and unitary groups. In the same year they calculated the ring of invariants of the symplectic group in [8] and their result showed that this ring of invariants is a graded complete intersection. There are several papers [[10], [11], [12], [15]] and theses [[3], [26]] which deal with the rings of invariants of orthogonal and unitary groups in low dimensional cases. In 2005 Kropholler, Mohseni Rajaei and Segal [24] found explicit generators and

relations for the rings of invariants of orthogonal groups over F_2 but the general case is still open. In 2006 Chu and Jow [14] computed rings of invariants of unitary groups. In the last two cases it was found that the rings of invariants are graded complete intersections. There is another unpublished paper [13] by Chu which deals with rings of invariants of orthogonal groups in odd characteristics. Chu did this work in 2007 but he discusses only two rings of invariants, and we know that when the dimension of V is even then up to isomorphism there are two orthogonal groups and corresponding to these two orthogonal groups we have two invariant rings up to isomorphism. Similarly when the dimension of the vector space V is odd then up to isomorphism there is only one orthogonal group and corresponding to this orthogonal group we have one invariant ring up to isomorphism. Thus by rings of invariants in odd characteristic we mean these two rings of invariants throughout the whole thesis.

The calculation of rings of invariants is important because once we calculate the generators of these rings and the relations among them we can understand the structure of these rings and so we can deal with these rings according to their properties.

In this thesis we do similar calculations to those which discussed above. The main research work in the thesis is in chapters 4, 5 and 6. Our motivation starts by considering subgroups of the general linear group which are similar to subgroups whose rings of invariants are already known.

In chapter 4 we consider the following groups and find rings of invariants.

$$\mathrm{Aut}(V,\xi) = \{g \in GL(V) : \xi(gv_1, gv_2) = \xi(v_1, v_2) \ \forall \ v_1, v_2 \in V\}$$

$$\mathrm{Aut}(V,H) = \{g \in GL(V) : H(gv_1, gv_2) = H(v_1, v_2) \ \forall \ v_1, v_2 \in V\}$$

In the first case V is a vector space over the finite field F_q and ξ is a singular alternating form on V while in the second case V is a vector space over the finite field F_{q^2} and H is a singular hermitian form on V. These two groups are similar to the symplectic and unitary groups: if the forms ξ and H are non-singular, then $\mathrm{Aut}(V,\xi)$ becomes the symplectic group and $\mathrm{Aut}(V,H)$ becomes the unitary group. As discussed above we know the rings of invariants of symplectic and unitary groups.

In particular we prove the following two results.

Theorem 4.7.2. *Suppose* $G = \mathrm{Aut}(V, \xi)$ *and* $x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}$ *is the dual basis of* V^* *corresponding to the basis* $e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+n}$ *of* V. *Let* $S = F_q[x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}]$ *and* $U = \mathrm{Rad}\xi = \langle e_1, \ldots, e_m \rangle$. *Then for* $y_i = \prod_{x \in (V/U)^*} (x_i - x)$, *we have* $S^G \cong F_q[y_1, \ldots, y_m]^{GL(U)} \otimes F_q[x_{m+1}, \ldots, x_{m+n}]^{S_P(V/U,\ \bar{\xi})}$.

Theorem 4.7.4. *Suppose* $G = \mathrm{Aut}(V, H)$ *and* $x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}$ *is the dual basis of* V^* *corresponding to the basis* $e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+n}$ *of* V. *Let* $S = F_{q^2}[x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}]$ *and* $W = \mathrm{Rad}H = \langle e_1, \ldots, e_m \rangle$. *Then for* $y_i = \prod_{x \in (V/W)^*} (x_i - x)$, *we have* $S^G \cong F_{q^2}[y_1, \ldots, y_m]^{GL(W)} \otimes F_{q^2}[x_{m+1}, \ldots, x_{m+n}]^{U(V/W,\ \bar{H})}$.

In chapter 5 we take a vector space V over the finite field F_q of dimension $2n$ together with a non-degenerate alternating form ξ of the following matrix

$$\begin{bmatrix} 0 & 1 & & & & & & \\ -1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & & 0 & 1 \\ & & & & & & -1 & 0 \end{bmatrix}$$

filled out with zeroes. We consider the following subgroup of the symplectic group $S_P(V, \xi)$:

$$G = \{g \in Sp(V, \xi) : gU = U\},$$

where U is a subspace of V. We consider the following two cases:

(i) $U = \langle e_1, e_2, \ldots, e_m \rangle$ where m is even and less than $2n$;

(ii) $U = \langle e_1, e_3, \ldots, e_{2n-1} \rangle$.

When we restrict the form ξ to U it is non-degenerate in the first case and degenerate in the second case. Again the above group is similar to the group

$$\{g \in GL(V) : gU = U\}$$

and the ring of invariants of this group is known. The following result gives ring of invariants S^G in the first case.

Theorem 5.2.1. *Let $x_1, \ldots, x_{2n}$ be the dual basis of V^* corresponding to the basis $e_1, \ldots, e_{2n}$ of V. Suppose $S = F_q[x_1, \ldots, x_{2n}]$ and $U = \langle e_1, e_2, \ldots, e_m \rangle$ as defined above. Then $S^G \cong F_q[x_1, x_2, \ldots, x_m]^{Sp(U,\ \xi|_U)} \otimes F_q[x_{m+1}, x_{m+2}, \ldots, x_{2n}]^{Sp(U^\perp,\ \xi|_{U^\perp})}$.*

In the second case we define a homomorphism $\phi : G \to GL(U)$ by $\phi(g) = g|_U$. By Witt's Lemma ϕ is onto. Therefore $G/\mathrm{Ker}\phi \cong GL(U)$. We take $N = \mathrm{Ker}\phi$ and $R = F_q[y_1, y_3, \ldots y_{2n-1}, x_2, x_4, \ldots, x_{2n}, \xi_1, \ldots \xi_{n-1}]$ where $y_i = \prod_{x \in (V/U)^*} (x_i - x)$ and $\xi_i = x_1 x_2^{q^i} - x_2 x_1^{q^i} + \cdots + x_{2n-1} x_{2n}^{q^i} - x_{2n} x_{2n-1}^{q^i}$. We prove the following results.

Lemma 5.3.1. *The following $n-1$ relations hold in R:*

$$\xi_i^{q^{n-i}} + \sum_{j=1}^{n} x_{2j}^{q^{n-i}} y_{2j-1} + \sum_{j=1}^{n-i} (-1)^{j+i+1} c_{n,n-j-i} \xi_j^{q^{n-j-i}} + \sum_{j=1}^{i-1} (-1)^j c_{n,n-j} \xi_{i-j}^{q^{n-i}} = 0$$

where $1 \le i \le n-1$.

Theorem 5.4.9. *Let $S = F_q[x_1, \ldots, x_{2n}]$ where $x_1, \ldots, x_{2n}$ is the dual basis of V^* corresponding to the basis $e_1, \ldots, e_{2n}$ of V. Then*

$$S^N = F_q[y_1, y_3, \ldots y_{2n-1}, x_2, x_4, \ldots, x_{2n}, \xi_1, \ldots \xi_{n-1}].$$

It may be possible to use it to find S^G by the formula $S^G = (S^N)^{G/N}$, but we do not know about S^G in this case. Thus this problem is still open.

Again in chapter 4 we consider the group

$$\mathrm{Aut}(V, Q) = \{g \in GL(V) : Q(gv) = Q(v)\ \forall\ v \in V\}$$

and find its ring of invariants. Here V is a vector space over the finite field F_q and Q is a singular quadratic form on V. Note that $\mathrm{Aut}(V, Q)$ is similar to the orthogonal group: if the form Q is non-singular then $\mathrm{Aut}(V, Q)$ becomes the orthogonal group. As discussed above the general case for the rings of invariants of the orthogonal groups is in progress. In particular we prove the following result.

Theorem 4.7.6. *Suppose* $G = \mathrm{Aut}(V, Q)$ *and* $x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}$ *is the dual basis of* V^* *corresponding to the basis* $e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+n}$ *of* V. *Let* $S = F_q[x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}]$ *and* $U = \mathrm{Rad}Q = \langle e_1, \ldots, e_m \rangle$. *Then for* $y_i = \prod_{x \in (V/U)^*} (x_i - x)$, *we have* $S^G \cong F_q[y_1, \ldots, y_m]^{GL(U)} \otimes F_q[x_{m+1}, \ldots, x_{m+n}]^{O(V/U,\ \bar{Q})}$.

From Theorem 4.7.2, Theorem 4.7.4, Theorem 4.7.6 and Theorem 5.2.1 it is clear that once we calculate the rings of invariants of the general linear, symplectic, unitary and orthogonal groups we can calculate the rings of invariants of $\mathrm{Aut}(V, \xi)$, $\mathrm{Aut}(V, H)$, $\mathrm{Aut}(V, Q)$ and $G = \{g \in Sp(V, \xi) : gU = U\}$ where $U = \langle e_1, e_2, \ldots, e_m \rangle$ as defined above.

In chapter 6 we generalize some of the results of [24]. In particular we prove the following result.

Theorem 6.7.1. *(i)* $\Omega_{2n}(X) = \sum_{i=0}^{2n} (\Lambda_{2n,i})^2 X^{(2^l)^i} + \delta$, *where* $\delta \in F_{2^l}[\xi_1, \xi_2, \ldots, \xi_{2n}]$.

(ii) In the ring S *we have* $\Omega_{2n}(X) = f_\infty^2 Q(X)$.

(iii) $\Omega_{2n}(X) = f_\infty^2 Q^-(X) Q^+(X)$, *and* $Q^-(X)$ *and* $Q^+(X)$ *are irreducible elements of the ring* $T^{(S_P(U,\ \bar{B}))}[X]$.

(iv) $f_\infty Q^-(X)$ *and* $f_\infty Q^+(X)$ *both belong to* $F_{2^l}[X, \xi_1, \ldots, \xi_{2n}]$.

Theorem 6.7.1 is motivated by Theorem 4.7.6, since we do not know about $F_q[x_{m+1}, \ldots, x_{m+n}]^{O(V/U,\ \bar{Q})}$ when $q = 2^l$, $l \geq 2$. There are two advantages of the above result. Firstly it helps us to calculate the ring of invariants over F_{2^l}, $l \geq 2$ as we mentioned in the beginning that this problem is still open. The particular case of Theorem 6.7.1 in [24] is used to prove the main results of that paper. Thus once we prove this result we can calculate the main results of [24] over any finite field of characteristic 2. In particular we can calculate S^G of Theorem 4.7.6 when $q = 2^l$, $l \geq 2$. Secondly, the proof of part (ii) of the above result appearing in [24] contains an error and we give an argument to correct this.

The thesis is organized as follows. Chapter 1 consists of known background material as well as basic results to be used in other chapters. In chapter 2, we give a brief summary of work previously done in this area. In particular we discuss the

rings of invariants of the general linear, symplectic and unitary groups, which were computed in [16], [8] and [14] respectively. We also discuss the rings of invariants of the orthogonal groups in odd characteristic, which were computed in [13]. In chapter 3, we describe some properties of the rings of invariants of the symplectic, unitary and orthogonal groups. In particular we can deduce from our presentations by generators and regular sequences of relators that our rings are Cohen-Macaulay and Gorenstein. In chapters 4, 5 and 6 we do our research work.

Chapter 1

Bilinear, hermitian, and quadratic forms

Throughout this thesis we consider commutative rings with identity.

In this chapter we present basic definitions, results and review some of the background material, which will be of value for our later pursuits.

1.1 Sesquilinear and quadratic forms

In this section V is an n-dimensional vector space over a field F and θ is an automorphism of F.

Definition 1.1.1. A *sesquilinear form* on V with respect to θ is a map $f : V \times V \to F$ such that, for all $u, v, w \in V$ and all $a \in F$:

$$f(u+v,w) = f(u,w) + f(v,w) \qquad f(au,v) = af(u,v)$$

$$f(u,v+w) = f(u,v) + f(u,w) \qquad f(u,av) = a^{\theta} f(u,v).$$

(i) The form f is said to be *bilinear* if $\theta = 1$.

(ii) The form f is said to be *hermitian* if θ is an involution and $f(u,v) = f(v,u)^{\theta}$ for all u, v in V.

Definition 1.1.2. We define the left and right *radicals* of f to be the subsets

$$\mathrm{LRad}f = \{u \in V : f(u, w) = 0 \ \forall \ w \in V\}$$

$$\mathrm{RRad}f = \{v \in V : f(w, v) = 0 \ \forall \ w \in V\}$$

respectively.

We define the radical of f to be

$$\mathrm{Rad}f = \{v \in V : f(u, v) = f(v, u) = 0 \ \forall \ u \in V\}.$$

Lemma 1.1.3. *The left and right radicals of f form subspaces of V.*

Proof. First note that $0 \in \mathrm{LRad}f$. Now suppose $u, v \in \mathrm{LRad}f$ and $\lambda \in F$, then $f(u - v, w) = f(u, w) - f(v, w) = 0$. Thus $u - v \in \mathrm{LRad}f$. Now $f(\lambda u, w) = \lambda f(u, w) = 0$. Therefore $\lambda u \in \mathrm{LRad}f$.

Clearly $0 \in \mathrm{RRad}f$. Let $u, v \in \mathrm{RRad}f$ and $\lambda \in F$, then $f(w, u - v) = f(w, u) - f(w, v) = 0$. Therefore $u - v \in \mathrm{RRad}f$. Now $f(w, \lambda u) = \lambda^{\theta} f(u, w) = 0$. Thus $\lambda u \in \mathrm{RRad}f$. □

Definition 1.1.4. A sesquilinear form f is said to be *non-degenerate or non-singular* if its left and right radicals are zero.

Definition 1.1.5. A bilinear form B is *symmetric* if $B(u, v) = B(v, u)$ for all u, v in V.

Definition 1.1.6. A bilinear form B is *skew symmetric* if $B(u, v) = -B(v, u)$ for all u, v in V.

Definition 1.1.7. A bilinear form B is *alternating* if $\forall \ v \in V \ B(v, v) = 0$.

It is easily shown that every alternating form is skew symmetric. See Lemma 1.2.10 for further information.

Definition 1.1.8. A bilinear form B is *reflexive* if and only if for all vectors $u, v \in V$

$$B(u, v) = 0 \text{ implies and is implied by } B(v, u) = 0.$$

The following result is a particular case of Theorem 6.1.3 in [6], the proof of which we present here.

Lemma 1.1.9. *A non-degenerate reflexive bilinear form is either symmetric or alternating.*

Proof. Let B be a non-degenerate reflexive bilinear form. Then, for any vectors u, v, w we have

$$B(u, B(u, v)w) = B(u, v)B(u, w) = B(u, w)B(u, v) = B(u, B(u, w)v),$$

and it follows that

$$B(u, B(u, v)w - B(u, w)v) = 0.$$

By reflexivity it follows that

$$B(B(u, v)w - B(u, w)v, u) = 0,$$

and therefore

$$B(u, v)B(w, u) = B(u, w)B(v, u). \tag{1.1}$$

We call a vector u *good* if there exists a vector v such that $B(u, v) = B(v, u) \neq 0$. From Equation (1.1) it follows that if u is a good vector then $B(u, w) = B(w, u)$ for all w. It follows that if u is good then all vectors w for which $B(u, w) \neq 0$ are good. Suppose that u is a good vector and v is any non-zero vector. Then since the form is non-degenerate, there exist vectors v' and v'' such that $B(u, v') \neq 0$ and $B(v, v'') \neq 0$. So v' is good. If $B(v, v')$ is non-zero then v is good. If $B(u, v'')$ is non-zero then it follows that v'' is good and therefore v is good. On the other hand, if both $B(v, v') = 0$ and $B(u, v'') = 0$ then $B(u, v' + v'')$ and $B(v, v' + v'')$ are both non-zero and hence again v is good. It follows that if there is a good vector then every non-zero vector is good and the form is symmetric.

Putting $u = v$ in Equation (1.1) we obtain the identity

$$B(u, u)(B(u, w) - B(w, u)) = 0.$$

and so, if there are no good vectors then $B(u, u) = 0$ for all u and the form is alternating. □

Definition 1.1.10. Suppose $\mathcal{B} = \{e_1, \ldots, e_n\}$ is an ordered basis for V and B is a bilinear form on V. Then B is completely determined by the $n \times n$ matrix

$$M_{\mathcal{B}} = (a_{ij}) = (B(e_i, e_j))$$

which is referred to as the matrix of the bilinear form B with respect to the ordered basis $\mathcal{B}$.

Observe that if $u = \sum c_i e_i$ and $v = \sum d_j e_j$, then

$$B(u, v) = \sum_i \sum_j c_i d_j B(e_i, e_j) = \sum_i c_i (\sum_j a_{ij} d_j) = [u]_{\mathcal{B}}^T M_{\mathcal{B}} [v]_{\mathcal{B}} \tag{1.2}$$

where $[u]_{\mathcal{B}}$ and $[v]_{\mathcal{B}}$ are the coordinate matrices of u and v respectively.

Notice also that B is symmetric if and only if its matrix $M_{\mathcal{B}} = (a_{ij})$ satisfies

$$a_{ij} = a_{ji}$$

for all $1 \leq i, j \leq n$, that is, if and only if $M_{\mathcal{B}}$ is a symmetric matrix. Similarly, B is alternate if and only if the matrix $M_{\mathcal{B}} = (a_{ij})$ satisfies

$$a_{ii} = 0, \qquad a_{ij} = -a_{ji} \quad (i \neq j);$$

such a matrix is referred to as alternate.

Theorem 1.1.11. *(Theorem 2.12 in [35]). Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ and $\mathcal{C} = \{f_1, \ldots, f_n\}$ be ordered bases for a vector space V. Then*

$$[v]_{\mathcal{C}} = M_{\mathcal{B},\mathcal{C}} [v]_{\mathcal{B}}$$

where the change of basis matrix $M_{\mathcal{B},\mathcal{C}}$ is the matrix whose ith column is $[e_i]_{\mathcal{C}}$.

Now let us see how the matrix of the bilinear form behaves with respect to a change of basis. Let $\mathcal{C} = \{f_1, \ldots, f_n\}$ be an ordered basis of V. Then by the above theorem, we have

$$\begin{aligned} B(u, v) &= ([u]_{\mathcal{C}}^T M_{\mathcal{C},\mathcal{B}}^T) M_{\mathcal{B}} (M_{\mathcal{C},\mathcal{B}} [v]_{\mathcal{C}}) \\ &= [u]_{\mathcal{C}}^T (M_{\mathcal{C},\mathcal{B}}^T M_{\mathcal{B}} M_{\mathcal{C},\mathcal{B}}) [v]_{\mathcal{C}}, \end{aligned}$$

and so

$$M_{\mathcal{C}} = M_{\mathcal{C},\mathcal{B}}^T M_{\mathcal{B}} M_{\mathcal{C},\mathcal{B}}.$$

This prompts the following definition:

Definition 1.1.12. Two matrices $A, C \in \mathcal{M}_n(F)$ are said to be *congruent* if there exists an invertible matrix P for which

$$A = PCP^T.$$

Let us summarize.

Theorem 1.1.13. *(Theorem 11.2 in [35]). If the matrix of a bilinear form B on V with respect to an ordered basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ is*

$$M_{\mathcal{B}} = (B(e_i, e_j))$$

then

$$B(u, v) = [u]_{\mathcal{B}}^T M_{\mathcal{B}} [v]_{\mathcal{B}}.$$

Furthermore, if $\mathcal{C} = \{f_1, \ldots, f_n\}$ is also an ordered basis for V, then we have

$$M_{\mathcal{C}} = M_{\mathcal{C},\mathcal{B}}^T M_{\mathcal{B}} M_{\mathcal{C},\mathcal{B}}$$

where $M_{\mathcal{C},\mathcal{B}}$ is the change of basis matrix from $\mathcal{C}$ to $\mathcal{B}$, whose ith column is $[f_i]_{\mathcal{B}}$.

Thus we have the following.

Theorem 1.1.14. *(Theorem 11.3 in [35]). Two matrices A and C represent the same bilinear form on V with respect to different choices of bases if and only if they are congruent.*

Definition 1.1.15. Let A be a matrix over a field F and θ an involution. Then A is said to be a *hermitian matrix* if $(A^T)^\theta = A$.

Now suppose $\{e_1, \ldots, e_n\}$ is a basis for V, $u = \sum_i c_i e_i$ and $v = \sum_i d_i e_i$. Let H be a hermitian form on V and $\widehat{H} = (H(e_i, e_j))$, then

$$H(u, v) = \sum_i \sum_j c_i H(e_i, e_j) d_j^\theta = c^T \widehat{H} d^\theta \tag{1.3}$$

where $c = (c_1, \ldots, c_n)^T$ and $d^\theta = (d_1^\theta, \ldots, d_n^\theta)^T$ in F^n. Since $H(u, v) = H(v, u)^\theta$ for all $u, v \in V$ we see that $\widehat{H} = (\widehat{H}^T)^\theta$, and we say that $\widehat{H}$ is a hermitian matrix. Conversely a hermitian matrix $\widehat{H}$ determines a hermitian form relative to the basis $\{e_1, \ldots, e_n\}$ for V by the above formula.

Definition 1.1.16. A *quadratic form* Q on V is a map $Q : V \to F$ such that:

(i) For all $\lambda \in F$ and all $v \in V$,

$$Q(\lambda v) = \lambda^2 Q(v);$$

(ii) The map

$$B : V \times V \to F$$

defined by

$$B(u, v) = Q(u + v) - Q(u) - Q(v)$$

is bilinear.

Here B is called the polarization of the quadratic form Q. It is always a symmetric form.

Now If Q is a quadratic form on a vector space V over a field F, then the pair (V, Q) is called a *quadratic space*.

Definition 1.1.17. If $Q : V \to F$ is a quadratic form, then its *radical* is defined as

$$\text{Rad}Q = \{v \in V : Q(u + v) - Q(u) - Q(v) = 0 \ \forall \ u \in V \text{ and } Q(v) = 0\}.$$

Lemma 1.1.18. Rad$Q$ *is a subspace of* V.

Proof. Clearly $0 \in \text{Rad}Q$. Let $v, w \in \text{Rad}Q$ and $\lambda \in F$, then

$$Q(u + v) - Q(u) - Q(v) = 0 \ \forall \ u \in V; \tag{1.4}$$

$$Q(u + w) - Q(u) - Q(w) = 0 \ \forall \ u \in V; \tag{1.5}$$

$$Q(v) = 0; \tag{1.6}$$

$$Q(w) = 0. \tag{1.7}$$

Now

$$Q(u+v-w)-Q(u)-Q(v-w) = Q(u+v)-Q(u)-Q(v)-(Q(u+w)-Q(u)-Q(w)),$$

and

$$Q(u+\lambda v)-Q(u)-Q(\lambda v) = \lambda(Q(u+v)-Q(u)-Q(v)).$$

Thus by using Equation (1.4) and Equation (1.5), we get

$$Q(u+v-w)-Q(u)-Q(v-w) = 0,$$

and

$$Q(u+\lambda v)-Q(u)-Q(\lambda v) = 0.$$

Now putting $u = -w$ in Equation (1.4), we have

$$Q(v-w)-Q(-w)-Q(v) = 0.$$

Also

$$Q(\lambda v) = \lambda^2 Q(v).$$

Therefore by using Equation (1.6) and Equation (1.7), we get $Q(v-w) = 0$ and $Q(\lambda v) = 0$. □

Definition 1.1.19. A quadratic form Q is said to be *non-degenerate or non-singular* if its radical is zero.

1.2 Some properties of finite fields

In this section we define finite fields. We give some useful results. These results have been taken from different sources: [25], [35] and [41].

Definition 1.2.1. A *finite field or Galois field* is a field which contains a finite number of elements. We usually denote finite field with q elements by F_q.

Definition 1.2.2. The *characteristic* of a finite field is the smallest number m such that m times the identity element is zero.

Before stating properties of finite fields we are going to define field extensions.

Definition 1.2.3. A *field extension* is a monomorphism $i : F \to E$, where F, E are fields.

Usually we identify F with its image $i(F)$, and in this case F becomes a subfield of E. We write E/F for an extension where F is a subfield of E.

Theorem 1.2.4. *(Theorem 6.1 in [41]). If E/F is a field extension, then the operation*

$$(\lambda, \mu) \mapsto \lambda\mu \quad (\lambda \in F,\ \mu \in E)$$

$$(u, v) \mapsto u + v \quad (u, v \in E)$$

turns E into a vector space over F.

Definition 1.2.5. The *degree* $[E : F]$ of a field extension E/F is the dimension of E considered as a vector space over F.

Definition 1.2.6. A *finite extension* is one whose degree is finite.

We now present some properties of finite fields which will be used in later sections.

Lemma 1.2.7. *(Theorem 2.2 in [25]). Let F be a finite field. Then F has p^n elements, where the prime p is the characteristic of F and n is the degree of F over its prime subfield F_p.*

Lemma 1.2.8. *(Corollary 20.9 in [41]). The multiplicative group $F_q^* = F_q \setminus \{0\}$ of a finite field F_q is cyclic.*

It follows that $a^q = a$ for all $a \in F_q$.

Lemma 1.2.9. *(Theorem 11.18 in [35]). Let F_q be a finite field with q elements.*

(i) If $\mathrm{char}(F_q) = 2$, then every element of F_q is a square.

(ii) If $\mathrm{char}(F_q) \neq 2$, then exactly half of the nonzero elements of F_q are squares. Moreover, if x is any nonsquare in F_q, then all nonsquare elements have the form r^2x for some $r \in F_q$.

Lemma 1.2.10. *(Lemma 11.1 in [35]). Let V be a vector space over the finite field F_q.*

(i) If $\mathrm{char}(F_q) = 2$, then a bilinear form on V is skew-symmetric if and only if it is symmetric. Furthermore, an alternating bilinear form is symmetric (and skew-symmetric).

(ii) If $\mathrm{char}(F_q) \neq 2$, then a bilinear form on V is skew-symmetric if and only if it is alternating.

Note that if the characteristic of the finite field F_q is not 2 then the quadratic form Q can be recovered from its polarization by the formula $Q(v) = \frac{1}{2}B(v, v)$ and there is a bijective correspondence between quadratic forms and symmetric bilinear forms. If F_q has characteristic 2, then the polarization is an alternating form from which the quadratic form cannot be recovered.

1.3 The dual vector space V^* and the symmetric algebra

This section is concerned with dual vector spaces and symmetric algebra. We give some results on these. These results have been taken from [27] and [35]. At the end of this section we prove a result which is old but we do not have a specific reference for.

Definition 1.3.1. Let V be a vector space over a field F. A mapping $\phi : V \to F$ is termed a *linear functional or linear form* on V if for $u, v \in V$ and every $a, b \in F$

$$\phi(au + bv) = a\phi(u) + b\phi(v).$$

In other words, a linear functional on V is a *linear mapping* from V into F.

The set of linear functionals on a vector space V over a field F is also a vector space over F with addition and multiplication defined by

$$(\phi + \delta)(v) = \phi(v) + \delta(v) \quad \text{and} \quad (\alpha\phi)(v) = \alpha\phi(v),$$

where ϕ and δ are linear functionals on V and $\alpha \in F$. This space is called the *dual space* of V and is denoted by V^*. Thus V^* has a dual space V^{**} called the *second dual* of V, which consists of all the linear functionals on V^*. Each $v \in V$ determines a specific element $\hat{v} \in V^{**}$ defined by

$$\hat{v}(\phi) = \phi(v).$$

Let us present some properties of dual spaces.

Definition 1.3.2. Suppose that V is finite dimensional, and let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of V. For each $1 \leq i \leq n$, we define a linear functional $x_i \in V^*$ by the orthogonality condition

$$x_i(e_j) = \delta_{ij} \quad \text{for} \quad j = 1, \ldots, n,$$

where δ_{ij}, known as the *Kronecker delta function*, is defined by

$$\delta_{ij} = \begin{cases} 1 & \text{if } \ i = j \\ 0 & \text{if } \ i \neq j. \end{cases}$$

Theorem 1.3.3. *(Theorem 3.11 in [35]). Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of V. Then the linear functionals $x_1, \ldots, x_n$ defined by*

$$x_i(e_j) = \delta_{ij} \quad \textit{for} \quad j = 1, \ldots, n$$

form a basis for the dual space V^*. This basis $\mathcal{B}^* = \{x_1, \ldots, x_n\}$ is called the dual basis for $\mathcal{B}$.

Corollary 1.3.4. *(See also corollary 3.12 in [35]). Let F be a field. If $\dim_F V < \infty$, then $\dim_F V^* = \dim_F V$.*

Theorem 1.3.5. *(Theorem 2.6 in [35]). Let V and W be vector spaces over F. Then $V \cong W$ if and only if $\dim_F V = \dim_F W$.*

It follows that $V \cong V^*$ whenever V has finite dimension.

Theorem 1.3.6. *(Theorem 11.4 in [27]). If V has finite dimension, then the mapping $v \mapsto \hat{v}$ is a natural isomorphism of V onto V^{**}.*

We are now going to define the symmetric algebra on a vector space V over a field F.

Definition 1.3.7. Let F be a field and V a vector space. The symmetric algebra on V, denoted by $S(V)$, is the quotient algebra over F of the tensor algebra $T(V)$ by the two sided ideal I generated by the elements $v \otimes u - u \otimes v$ of $T(V)$, where $u, v \in V$.

If V has basis $e_1, \ldots, e_n$ then $S(V)$ is isomorphic to the polynomial ring $F[e_1, \ldots, e_n]$. We shall denote the symmetric algebra on V^* by $F[V]$.

We now describe some properties of the symmetric algebra on V^* which will be used in later chapters.

Definition 1.3.8. Let V be a vector space over a finite field F_q where $q = p^n$ for some prime p. We define the *Frobenius map* $\phi : F_q[V] \to F_q[V]$ by $\phi(x) = x^p$.

Lemma 1.3.9. *The Frobenius map, ϕ is a monomorphism.*

Proof. Let $x, y \in F_q[V]$. Then

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y).$$

Also

$$\phi(x+y) = (x+y)^p = x^p + px^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + pxy^{p-1} + y^p \qquad (1.8)$$

by the binomial theorem. We claim that the binomial coefficient

$$\binom{p}{r}$$

is divisible by p if $1 \leq r \leq p-1$. To prove this, observe that the binomial coefficient is an integer, and

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}$$

The factor p in the numerator cannot cancel unless $r = 0$ or p.

Hence the sum in Equation (1.8) reduces to its first and last terms, so

$$\phi(x+y) = x^p + y^p = \phi(x) + \phi(y).$$

Therefore, ϕ is a homomorphism. Also Ker$\phi = 0$ because the symmetric algebra is an integral domain. □

Corollary 1.3.10. *The map*

$$\phi^{'} : F_q[V] \to F_q[V]$$

defined by

$$x \mapsto x^q$$

where $q = p^n$ for prime p, is a monomorphism.

Proof. Follows from the above Lemma. □

Definition 1.3.11. Given a basis $x_1, \ldots, x_n$ of V^* corresponding to the basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of V. The general form of the quadratic form is

$$Q = \sum_i \sum_j a_{ij} x_i x_j.$$

Thus

$$Q = x^T M x$$

where M is the matrix of the coefficients of the form and x is the column vector with components $x_1, \ldots, x_n$.

Now let $v = \sum d_k e_k$. If we form $Q(v) = B(v, v)$ we find from Equation (1.2) that

$$\begin{aligned} Q(v) &= \sum_i \sum_j B(e_i, e_j) d_i d_j \\ &= \sum_i \sum_j B(e_i, e_j) x_i(v) x_j(v). \end{aligned}$$

Thus, we have

$$Q = \sum_i \sum_j a_{ij} x_i x_j$$

where $a_{ij} = B(e_i, e_j)$.

1.4 Equivalence of bilinear, hermitian and quadratic forms

Definition 1.4.1. Let X be a set and let $\sim$ be an equivalence relation on X. If $x \in X$, then the *equivalence class* of x modulo $\sim$ is the set $[x]_\sim$, defined as follows:

$$[x]_\sim = \{y \in X : y \sim x\}.$$

Definition 1.4.2. A *right group action* of the group G on the set X is determined by a function $X \times G \to X$, where we write $(x, g) \mapsto x \cdot g$, satisfying the two axioms:

$$x \cdot (gh) = (x \cdot g) \cdot h$$

and

$$x \cdot 1 = x \quad (x \in X, \quad g, h \in G).$$

Lemma 1.4.3. *Let G act on X. Define a relation $\sim$ on X by $x \sim y$ if and only if there exists $g \in G$ such that $x \cdot g = y$. Then $\sim$ is an equivalence relation.*

Proof. Firstly, $x \sim x$ as $x \cdot 1 = x$. Now let $x \sim y$. Then there exists $g \in G$ such that $x \cdot g = y$. Thus $x = y \cdot g^{-1}$, so $y \sim x$. Now let $x \sim y$ and $y \sim z$. Then there exist $g, h \in G$ such that $x \cdot g = y$ and $y \cdot h = z$. Now $x \cdot (gh) = (x \cdot g) \cdot h = y \cdot h = z$. So we get $x \sim z$. □

Thus if G acts on X, then X is partitioned into blocks called *orbits*. We write $\mathrm{Orb}(x)$ for the orbit of $x \in X$. These are the equivalence classes under the above relation.

Definition 1.4.4. Let G act on X and let $x \in X$. Define the *stabilizer* of x in G to be

$$G_x = \{g \in G : x \cdot g = x\}.$$

It is easy to see that the stabilizer of x is a subgroup of G.

Theorem 1.4.5. *(Theorem 3.19 in [36]). Let G act on the set X. Then for $x \in X$,*

$$|\mathrm{Orb}(x)| = |G : G_x|.$$

The above theorem is called the *orbit stabilizer theorem*.

Definition 1.4.6. If V is an n-dimensional vector space over a field F, then $GL(V)$ denotes the *general linear group* of V, i.e the group of all invertible linear transformations on V.

Choosing a basis for V provides an isomorphism of $GL(V)$ with the group $GL(n, F)$ of all invertible $n \times n$ matrices over F.

Definition 1.4.7. Two quadratic forms Q and $Q^{'}$ on a vector space V over a field F are said to be *equivalent* if there exists $g \in GL(V)$ such that $Q^{'}(v) = Q(gv)$ for all $v \in V$.

Now let $v = \sum d_k e_k$. From Definition 1.3.11, we have

$$Q(v) = [v]^T M[v]$$

where M is the matrix of the coefficients of the form and $[v]$ is the column vector with components $d_1, \ldots, d_n$. Therefore

$$\begin{aligned} Q^{'}(v) &= Q(gv) \\ &= [gv]^T M[gv] \\ &= [v]^T([g]^T M[g])[v]. \end{aligned}$$

Thus in other words $Q^{'}$ is equivalent to Q if $Q^{'}$ is obtained from Q by replacing the matrix M by its conjugate $[g]^T M[g]$.

Definition 1.4.8. Two bilinear forms B and $B^{'}$ on a vector space V over a field F are said to be *equivalent* if there exists $g \in GL(V)$ such that $B^{'}(u, v) = B(gu, gv)$ for all $u, v \in V$.

Now from Equation (1.2)

$$B(u, v) = [u]_{\mathcal{B}}^T M_{\mathcal{B}}[v]_{\mathcal{B}}.$$

Therefore we have

$$\begin{aligned} B^{'}(u, v) &= B(gu, gv) \\ &= [gu]_{\mathcal{B}}^T M_{\mathcal{B}}[gv]_{\mathcal{B}} \\ &= [u]_{\mathcal{B}}^T([g]_{\mathcal{B}}^T M_{\mathcal{B}}[g]_{\mathcal{B}})[v]_{\mathcal{B}}. \end{aligned}$$

In other words $B^{'}$ is equivalent to B if $B^{'}$ is obtained from B by replacing the matrix $M_{\mathcal{B}}$ by its conjugate $[g]_{\mathcal{B}}^{T} M_{\mathcal{B}} [g]_{\mathcal{B}}$.

Definition 1.4.9. Two hermitian forms H and $H^{'}$ on a vector space V over a field F are said to be *equivalent* if there exists $g \in GL(V)$ such that $H^{'}(u, v) = H(gu, gv)$ for all $u, v \in V$.

Now from Equation (1.3)

$$H(u, v) = [u]^{T} \widehat{H} [v]^{\theta}$$

where $[u]$ and $[v]$ are the coordinate matrices of u and v respectively. Thus

$$\begin{aligned} H^{'}(u, v) &= H(gu, gv) \\ &= [gu]^{T} \widehat{H} [gv]^{\theta} \\ &= [u]^{T} ([g]^{T} \widehat{H} [g]^{\theta}) [v]^{\theta}. \end{aligned}$$

In other words $H^{'}$ is equivalent to H if $H^{'}$ is obtained from H by replacing the matrix $\widehat{H}$ by the matrix $[g]^{T} \widehat{H} [g]^{\theta}$.

Lemma 1.4.10. *Let V be an n-dimensional vector space over a finite field F of order q and characteristic p. Then*

(i) V admits a non-degenerate alternating form B if and only if n is even, in which case B is unique up to equivalence.

(ii) V admits a hermitian form H if and only if q is square with automorphism θ of V defined by $\theta(x) = x^{p^m}$. If H is non-degenerate then H is unique up to equivalence.

(iii) If n is even V admits exactly two equivalence classes of non-degenerate quadratic forms.

(iv) If n is odd then V admits a non-degenerate quadratic form precisely when p is odd, in which case there are two equivalence classes of forms. All forms are equivalent up to scalar multiplication.

Proof. Follows from Theorem 21.6 in [1]. □

Remark 1.4.11. In the situation of (iii) and (iv), there are two types of non-degenerate quadratic forms called +type and −type.

Definition 1.4.12. A field F is said to be *perfect* if either:

(i) F has characteristic zero or

(ii) F has characteristic p, and every element of F has a pth root in F.

Proposition 1.4.13. *(Proposition 7.29 in [7]). Every finite field is perfect.*

This can also be deduced from Lemma 1.3.9.

Theorem 1.4.14. *Suppose that F is a perfect field of characteristic 2 and Q is a non-degenerate quadratic form on V over F. Let V have basis $e_1, \ldots, e_n$ and suppose that V^* has corresponding basis $x_1, \ldots . x_n$. Then Q takes one of the following three forms:*

(i) If $n = 2m + 1$ is odd, then

$$Q = x_1x_{m+1} + x_2x_{m+2} + \cdots + x_mx_{2m} + x_{2m+1}^2.$$

(ii) If $n = 2m$ is even, then either

(a) $Q = x_1x_{m+1} + x_2x_{m+2} + \cdots + x_mx_{2m}$

or

(b) $Q = x_1x_m + x_2x_{m+1} + \cdots + x_{m-1}x_{2m-2} + x_{2m-1}^2 + x_{2m}x_{2m-1} + bx_{2m}^2$,

with $x_{2m-1}^2 + x_{2m-1} + b$ irreducible in $F[x_{2m-1}]$.

Proof. Follows from Theorem 12.9 in [20]. □

Remark 1.4.15. The quadratic forms in (a) and (b) are said to be of +type and −type respectively.

1.5 Symplectic, unitary and orthogonal groups

In this section we define symplectic, unitary and orthogonal groups. We give the orders of these groups along with the order of the general linear group in any characteristic. We shall use these orders in chapter 6.

Definition 1.5.1. Let ξ be a non-degenerate alternating form on a vector space V of even dimension n over a field F. Then the *symplectic group* is defined to be

$$S_P(V,\xi) = \{g \in GL(V) : \xi^g = \xi\},$$

where ξ^g is defined by

$$\xi^g(u,v) = \xi(gu,gv).$$

That is, $S_P(V,\xi)$ is the largest subgroup of $GL(V)$ under which ξ is invariant.

Definition 1.5.2. Let F be a field and θ an automorphism of F which is an involution. Suppose H is a non-degenerate hermitian form on a vector space V of dimension n over the field F. Then the *unitary group* is defined to be

$$U(V,H) = \{g \in GL(V) : H^g = H\},$$

where H^g is defined by

$$H^g(u,v) = H(gu,gv).$$

That is, $U(V,H)$ is the largest subgroup of $GL(V)$ under which H is invariant.

Definition 1.5.3. Let Q be a non-singular quadratic form on a vector space V of dimension n over a field F. Then the *orthogonal group* is defined to be

$$O(V,Q) = \{g \in GL(V) : Q^g = Q\},$$

where Q^g is defined by

$$Q^g(v) = Q(gv).$$

That is, $O(V,Q)$ is the largest subgroup of $GL(V)$ under which Q is invariant.

Now from Lemma 1.4.10 and Theorem 1.4.14, it is clear that up to isomorphism there is only one symplectic group and one unitary group corresponding to each space V. Therefore we can write $S_P(n, F)$ and $U(n, F)$ for the symplectic and unitary groups corresponding to a vector space of dimension n. There is one orthogonal group up to isomorphism when the dimension of V is odd and so we can write $O(n, F)$ for the corresponding orthogonal group. There are two orthogonal groups up to isomorphism when the dimension of V is even and so we can write $O^+(n, F)$ and $O^-(n, F)$ for the corresponding two orthogonal groups.

In the following results F denotes a field.

Proposition 1.5.4. *If $|F| = q$ is finite, then*

$$|GL(n, F)| = q^{n(n-1)/2} \prod_{k=1}^{n} (q^k - 1).$$

Proof. Follows from Proposition 1.1 in [20]. □

Theorem 1.5.5. *If $|F| = q$ is finite, then*

$$|S_P(n, F)| = q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1)$$

where $n = 2m$.

Proof. Follows from Theorem 3.12 in [20]. □

Theorem 1.5.6. *(Theorem 11.28 in [20]). If $|F| = q^2$ is finite and $dim V = n$, then*

$$|U(n, F)| = q^{n(n-1)/2} \prod_{j=1}^{n} (q^j - (-1)^j).$$

Theorem 1.5.7. *(Theorem 14.2 in [20]). If F is a perfect field of characteristic 2 and V is a quadratic space of odd dimension $n = 2m+1$, then $O(n, F) \cong S_P(2m, F)$.*

Corollary 1.5.8. *If $|F| = 2^l$ and $dim V = 2m + 1$, then*

$$|O(2m + 1, F)| = (2^l)^{m^2} \prod_{i=1}^{m} ((2^l)^{2i} - 1).$$

Proof. Follows from Proposition 1.4.13, Theorem 1.5.5 and Theorem 1.5.7. □

Theorem 1.5.9. *(Theorem 9.11 in [20]). Suppose* $|F| = q$ *and* $charF \neq 2$. *Then*

(i) $|O^+(2k, F)| = 2q^{k(k-1)}(q^k - 1)\prod_{i=1}^{k-1}(q^{2i} - 1)$.

(ii) $|O^-(2k, F)| = 2q^{k(k-1)}(q^k + 1)\prod_{i=1}^{k-1}(q^{2i} - 1)$.

(iii) $|O(2k + 1, F)| = 2q^{k^2}\prod_{i=1}^{k}(q^{2i} - 1)$.

Note that the orders of the orthogonal groups in odd characteristic are also given in Theorem 6.17 in [21].

Theorem 1.5.10. *Suppose that* $|F| = 2^l$ *and* Q *is a non-singular quadratic form on a vector space* V *of even dimension* n *over the field* F. *If* Q *is a quadratic form of* $+$type, *then*

$$|O^+(n, F)| = 2(2^l)^{\frac{n(n-2)}{4}}((2^l)^{\frac{n}{2}} - 1)\prod_{i=1}^{\frac{n-2}{2}}((2^l)^{2i} - 1).$$

If Q *is a quadratic form of* $-$type, *then*

$$|O^-(n, F)| = 2(2^l)^{\frac{n(n-2)}{4}}((2^l)^{\frac{n}{2}} + 1)\prod_{i=1}^{\frac{n-2}{2}}((2^l)^{2i} - 1).$$

Proof. Follows from Theorem 14.48 in [20]. □

Chapter 2

Invariant rings of symplectic, unitary & orthogonal groups

Let V be a vector space over the finite field F_q. Let $S = F_q[V]$ be the symmetric algebra on the dual V^* of V. In this chapter we define the invariant ring S^G where $G \leq GL(V)$. We discuss the invariant rings of the symplectic, unitary and orthogonal groups. The ring of invariants of the symplectic group was calculated by Carlisle and Kropholler in [8]. The ring of invariants of the unitary group was computed by Chu and Jow in [14]. The ring of invariants of the orthogonal group in odd characteristic was computed by Chu in [13]. Here we give a brief summary.

2.1 Invariant ring S^G where $G \leq GL(V)$

The group $G \leq GL(V)$ acts on V as follows:

$$g \cdot v = g(v).$$

This is a left action of G on V and this gives a right action of G on V^* as follows:

$$x^g(v) = x(g \cdot v).$$

The action of G on V^* extends to an action on S by ring automorphism as follows:

(i) $(y + z)^g = y^g + z^g$;

(ii) $(yz)^g = y^g z^g$;

(iii) $1^g = 1$.

We define the *invariant ring* as follows:

$$S^G = \{f \in S : f^g = f \ \forall \ g \in G\}.$$

The invariant ring of the general linear group $GL(V)$ was computed early in the 20th century by Dickson in [16]. For a more modern treatment see Wilkerson [43]. It was found to be a graded polynomial algebra on certain generators $\{c_{V,i}\}$, called the Dickson invariants.

Definition 2.1.1. The *Dickson polynomial* is defined as

$$D_V(X) = \prod_{x \in V^*} (X - x).$$

Here V is a vector space of dimension n over F_q where $q = p^r$ and p is a prime. It should be noted that $D_V(X)$ is invariant under the action of $GL(V)$ as any element $g \in GL(V)$ merely permutes the elements of V^*. It follows that the coefficients of powers of X are also invariants. The coefficients are the Dickson invariants. Note that $D_V(X) \in F_q[V][X]$.

The following result is similar to Proposition 1.1 of [43]. In Proposition 1.1 instead of a finite field F_q the author considers a field F containing the F_q-vector space V. Here we do the same calculations over the finite field F_q.

Lemma 2.1.2. *Let* $D_V(X) = \prod_{x \in V^*} (X - x)$. *Then*

$$D_V(X) = \sum_{i=0}^{n} (-1)^{n-i} c_{V,i} X^{q^i}$$

where $c_{V,i} \in F_q[V]$.

Proof. Let $e_1, \ldots, e_n$ be a basis of V and suppose $x_1, \ldots, x_n$ is the dual basis of V^* corresponding to the basis $e_1, \ldots, e_n$ of V. In this proof, we write $D_n(X)$ for $D_V(X)$

and $D_{n-1-j}(X)$ for $D_{(V/\langle e_n,\ldots,e_{n-j}\rangle)}$, where $0 \leq j \leq n$. Consider the following matrix.

$$\mathcal{F}_n(X) = \begin{bmatrix} x_1 & x_1^q & x_1^{q^2} & \cdots & x_1^{q^n} \\ x_2 & x_2^q & x_2^{q^2} & \cdots & x_2^{q^n} \\ x_3 & x_3^q & x_3^{q^2} & \cdots & x_3^{q^n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^q & x_n^{q^2} & \cdots & x_n^{q^n} \\ X & X^q & X^{q^2} & \cdots & X^{q^n} \end{bmatrix}.$$

Now by taking the determinant of both sides, we have

$$\det(\mathcal{F}_n(X)) = \begin{vmatrix} x_1 & x_1^q & x_1^{q^2} & \cdots & x_1^{q^n} \\ x_2 & x_2^q & x_2^{q^2} & \cdots & x_2^{q^n} \\ x_3 & x_3^q & x_3^{q^2} & \cdots & x_3^{q^n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^q & x_n^{q^2} & \cdots & x_n^{q^n} \\ X & X^q & X^{q^2} & \cdots & X^{q^n} \end{vmatrix}.$$

Let $x \in V^*$, then $x = \sum_{i=1}^n a_i x_i$ where $a_i \in F_q$ and

$$\det(\mathcal{F}_n(X)) = \begin{vmatrix} x_1 & x_1^q & \cdots & x_1^{q^n} \\ x_2 & x_2^q & \cdots & x_2^{q^n} \\ x_3 & x_3^q & \cdots & x_3^{q^n} \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^q & \cdots & x_n^{q^n} \\ X - \sum a_i x_i & X^q - \sum a_i x_i^q & \cdots & X^{q^n} - \sum a_i x_i^{q^n} \end{vmatrix}.$$

By the linearity of the map $x \mapsto x^{q^i}$ (See Lemma 1.2.8 and Corollary 1.3.10), we get

$$\det(\mathcal{F}_n(X)) = \begin{vmatrix} x_1 & x_1^q & \cdots & x_1^{q^n} \\ x_2 & x_2^q & \cdots & x_2^{q^n} \\ x_3 & x_3^q & \cdots & x_3^{q^n} \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^q & \cdots & x_n^{q^n} \\ X - x & (X-x)^q & \cdots & (X-x)^{q^n} \end{vmatrix}.$$

It follows from above that each $x \in V^*$ is a root of $\det(\mathcal{F}_n(X))$. Let $\Delta_n(X) = \det(\mathcal{F}_n(X))$, then

$$\Delta_n(X) = \Delta_{n-1}(x_n)D_n(X).$$

Next we need to show that $\Delta_{n-1}(x_n) \neq 0$. For this we use induction on n. For $n = 1$, $\Delta_0(x_1) = x_1$ and $x_1 \neq 0$. Suppose the statement is true for vector spaces of dimension less than n. Then

$$\Delta_{n-1}(X) = \Delta_{n-2}(x_{n-1})D_{n-1}(X) \neq 0.$$

But the roots of $\Delta_{n-1}(X)$ are the roots of the $n-1$ dimensional subspace of V generated by $x_1, \ldots, x_{n-1}$. It follows that x_n is not a root of $\Delta_{n-1}(X)$. Thus $\Delta_{n-1}(x_n) \neq 0$. Now define $\Upsilon_{n,i}$ to be the matrix obtained from $\mathcal{F}_n(X)$ by removing the $(n+1)$th row and $(i+1)$th column. Then

$$\Delta_n(X) = \sum_{i=0}^{n} (-1)^{n-i} \det \Upsilon_{n,i} X^{q^i}.$$

Therefore it follows that

$$D_n(X) = \sum_{i=0}^{n} (-1)^{n-i} c_{V,i} X^{q^i}$$

where $c_{V,i} = \dfrac{\det \Upsilon_{n,i}}{\det \Upsilon_{n,n}}$. □

Theorem 2.1.3. *(Theorem 8.1.5 in [39]).*

$$F_q[V]^{GL(V)} = F_q[c_{V,n-1}, \ldots, c_{V,0}]$$

where $\deg c_{V,i} = q^n - q^i$ *for* $i = 1, \ldots, n$.

2.2 The invariant ring of the symplectic group

Let $q = p^r$ where p is a prime and suppose V is a vector space over F_q of dimension $2n$, with basis $e_1, \ldots, e_{2n}$. Let G be the finite symplectic group $S_P(2n, F_q)$. In this section we describe the calculation by Carlisle and Kropholler of the invariant ring $F_q[V]^{S_P(2n,\ F_q)}$.

Definition 2.2.1. If $x_1, \ldots, x_{2n}$ is the basis of V^* dual to $e_1, \ldots, e_{2n}$, then we define

$$\xi_i = x_1 x_2^{q^i} - x_2 x_1^{q^i} + x_3 x_4^{q^i} - x_4 x_3^{q^i} + \cdots + x_{2n-1} x_{2n}^{q^i} - x_{2n} x_{2n-1}^{q^i}.$$

The following results have been taken from [32] in which the author considers finite fields with odd characteristic but the results are still true when the characteristic of the field is even.

Proposition 2.2.2. *(Proposition 2.1 in [32]). For any natural number $i \in \mathbb{N}$ we have $\xi_i \in F_q[V]^{S_P(2n,\ F_q)}$.*

Lemma 2.2.3. *(Lemma 2.2 in [32]). $S_P(2n, F_q) = \{g \in GL(2n, F_q) : \xi_1^g = \xi_1\}$.*

Theorem 2.2.4. *(Theorem 6.4 in [32]). The ring $F_q[V]^{S_P(2n,\ F_q)}$ is generated by the elements*

$$c_{V,\ n}, \ldots, c_{V,\ 2n-1}, \xi_1, \ldots, \xi_{2n-1}$$

subject only to the following relations:

$$\sum_{j=0}^{i-1} (-1)^j \xi_{i-j}^{q^j} c_{V,j} = \sum_{j=i+1}^{2n} (-1)^j \xi_{j-i}^{q^i} c_{V,j} \quad (1 \leq i \leq n-1).$$

2.3 The invariant ring of the unitary group

Let V be a vector space of dimension n over the finite field F_{q^2}. Let V have basis $e_1, \ldots, e_n$ and suppose that V^* has the corresponding basis $x_1, \ldots, x_n$. Set $\xi = x_1^{q+1} + \cdots + x_n^{q+1}$. In [14] the authors simply state that this is a hermitian form, however this statement needs to be amplified because there is no immediate connection between this function of one variable and the sesquilinear Definition 1.1.1 which is a function of two variables. For this reason we explain in more detail, the correspondence between the two views of hermitian form. This ξ determines a function

$$h : V \to F_{q^2}$$

defined by

$$v \to x_1^{q+1}(v) + \cdots + x_n^{q+1}(v).$$

We shall show that h determines a hermitian form on V in both odd and even characteristics. The idea comes from page 87 of [20]. In [20] the author considers the field of complex numbers and do the calculations. Here we do the same calculations over the finite field F_{q^2}.

If Char$F_{q^2} \neq 2$ choose $j \in F_{q^2} \setminus \{0\}$ such that $j^q = -j$. Now define

$$H : V \times V \to F_{q^2}$$

by

$$H(u,v) = \frac{1}{4}(h(u+v) - h(u-v) + \frac{1}{j}(h(u+jv) - h(u-jv))).$$

If Char$F_{q^2} = 2$ choose $\lambda \in F_{q^2} \setminus \{0\}$ such that $\lambda^q = \lambda^{-1} \neq \lambda$. Now define

$$H : V \times V \to F_{q^2}$$

by

$$H(u,v) = \frac{1}{\lambda + \lambda^{-1}} h(u+v) + \frac{1}{1+\lambda+\lambda^2+\lambda^3}(\lambda h(u+\lambda v) + \lambda^2 h(u+\lambda^{-1}v)).$$

Let $u = \sum a_i e_i$ and $v = \sum b_i e_i$, then in both cases we get

$$H(u,v) = a_1 b_1^q + \cdots + a_n b_n^q.$$

We can easily check that H is a non-singular hermitian form on V. In this section we describe explicit generators and relations for the ring of invariants $F_{q^2}[V]^{U(n,\ F_{q^2})}$. Suppose $\xi_{n,i} := x_1^{q^{2i+1}+1} + \cdots + x_n^{q^{2i+1}+1}$. It is known that $\xi_{n,i} \in F_{q^2}[V]^{U(n,\ F_{q^2})}$ and it was computed in [9] that $F_{q^2}(V)^{U(n,\ F_{q^2})} = F_{q^2}(\xi_{n,0}, \ldots, \xi_{n,n-1})$. First of all we construct a polynomial, which we will denote by G_n'.

We consider the following matrix:

$$N = \begin{bmatrix} X_0 & X_0^q & X_1^q & X_2^q & X_3^q & \cdots \\ X_1 & X_0^{q^2} & X_0^{q^3} & X_1^{q^3} & X_2^{q^3} & \cdots \\ X_2 & X_1^{q^2} & X_0^{q^4} & X_0^{q^5} & X_1^{q^5} & \cdots \\ X_3 & X_2^{q^2} & X_1^{q^4} & X_0^{q^6} & X_0^{q^7} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

where (i,j)-entry of the above matrix is

$$\begin{cases} X_{j-i-1}^{q^{2i-1}}, & i<j; \\ X_{i-j}^{q^{2j-2}}, & i \geq j. \end{cases}$$

Let F_n be the n-minor obtained by the first n columns and rows of N, then clearly $F_n \in F_q[X_0,\ldots,X_{n-1}]$. For example

$$F_1 = X_0 \quad \text{and} \quad F_2 = X_0^{q^2+1} - X_0^q X_1.$$

Let $F_n^{'}$ be the n-minor obtained from the first n columns and the second row to the $(n+1)$th row of N, then clearly $F_n^{'} \in F_q[X_0,\ldots,X_n]$. For example

$$F_1^{'} = X_1 \quad \text{and} \quad F_2^{'} = X_1^{q^2+1} - X_0^{q^2} X_2.$$

Let $G_n := F_n^{q^2-q+1} - F_n^{'}$ and define $G_{-2}^{'} = G_{-1}^{'} = 1, G_0^{'} = X_0$ and

$$G_n^{'} := G_n / G_{n-3}^{'q^3}, \quad n \geq 1.$$

We are now going to state a result which confirms that $G_n^{'}$ is a polynomial.

Theorem 2.3.1. *(Lemma 1.3 in [14]).*

(i) $G_{n-3}^{'q^3} | G_n$, *for* $n \geq 1$;

(ii) $G_n^{'}$ *is irreducible or a unit for* $n \geq -2$;

(iii) $F_n = G_{n-2}^{'q} G_{n-1}^{'}$ *for* $n \geq 0$.

We now describe a connection between two results. These results concern determinants and are very important in invariant theory.

Definition 2.3.2. Suppose M is an $m \times n$ matrix, S a subset of $\{1,2,\ldots,m\}$ and T a subset of $\{1,2,\ldots,n\}$. Define $M_{S;T}$ to be the submatrix of M obtained by removing the rows in S and the columns in T. If $S = \{i\}$ and $T = \{j\}$, we take M_{ij} instead of $M_{S;T}$.

Lemma 2.3.3. *(Lemma 2 on page 108 in [19]). For any $p \times p$ matrices M and N, and $1 \leq k \leq p$,*

$$\det(M) \cdot \det(N) = \sum \det(M^{'}) \cdot \det(N^{'})$$

where the sum is over all pairs $(M^{'}, N^{'})$ of matrices obtained from M and N by interchanging a fixed set of k columns of N with any k columns of M, preserving the ordering of the columns.

Example 2.3.4. *Let*

$$M = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \text{ and } N = \begin{bmatrix} 5 & 2 \\ 6 & 9 \end{bmatrix}.$$

Then

$$\det M \cdot \det N = 66.$$

By fixing the first column of N we get

$$\sum \det(M^{'}) \cdot \det(N^{'}) = \begin{vmatrix} 2 & 5 \\ 4 & 6 \end{vmatrix} \begin{vmatrix} 1 & 2 \\ 3 & 9 \end{vmatrix} + \begin{vmatrix} 5 & 1 \\ 6 & 3 \end{vmatrix} \begin{vmatrix} 2 & 2 \\ 4 & 9 \end{vmatrix}$$
$$= 66.$$

Theorem 2.3.5. *Let R be a ring and $M \in M_n(R)$. Let $N \in M_{n-2}(R)$ be the matrix obtained by deleting the first row, the last row, the first column and the last column from M. Then*

$$\det(M) \cdot \det(N) = |M_{nn}| \cdot |M_{11}| - |M_{n1}| \cdot |M_{1n}|.$$

Proof. Suppose n is even and let

$$M = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1\ n-1} & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2\ n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-1} & a_{n-1\ n} \\ a_{n1} & a_{n2} & \dots & a_{n\ n-1} & a_{nn} \end{bmatrix}$$

and

$$N = \begin{bmatrix} a_{22} & a_{23} & \dots & a_{2\ n-2} & a_{2\ n-1} \\ a_{32} & a_{33} & \dots & a_{3\ n-2} & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2\ 2} & a_{n-2\ 3} & \dots & a_{n-2\ n-2} & a_{n-2\ n-1} \\ a_{n-1\ 2} & a_{n-1\ 3} & \dots & a_{n-1\ n-2} & a_{n-1\ n-1} \end{bmatrix}.$$

Now $\det M \cdot \det N =$

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1\ n-1} & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2\ n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-1} & a_{n-1\ n} \\ a_{n1} & a_{n2} & \dots & a_{n\ n-1} & a_{nn} \end{vmatrix} \begin{vmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & a_{22} & \dots & a_{2\ n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a_{n-1\ 2} & \dots & a_{n-1\ n-1} & 0 \\ 0 & 0 & \dots & 0 & 1 \end{vmatrix}.$$

By the above lemma for $k = n-1$, we have $\det M \cdot \det N =$

$$\begin{vmatrix} a_{11} & 0 & \dots & 0 & 0 \\ a_{21} & a_{22} & \dots & a_{2\ n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-1} & 0 \\ a_{n1} & 0 & \dots & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & a_{12} & \dots & a_{1\ n-1} & a_{1n} \\ 0 & a_{22} & \dots & a_{2\ n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a_{n-1\ 2} & \dots & a_{n-1\ n-1} & a_{n-1\ n} \\ 0 & a_{n2} & \dots & a_{n\ n-1} & a_{nn} \end{vmatrix}$$

$+ \cdots +$

$$\begin{vmatrix} a_{11} & 1 & 0 & \dots & 0 & 0 \\ a_{21} & 0 & a_{22} & \dots & a_{2\ n-2} & a_{2\ n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 1} & 0 & a_{n-1\ 2} & \dots & a_{n-1\ n-2} & a_{n-1\ n-1} \\ a_{n1} & 0 & 0 & \dots & 0 & 0 \end{vmatrix} \begin{vmatrix} a_{12} & a_{13} & \dots & a_{1n} & 0 \\ a_{22} & a_{23} & \dots & a_{2n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 2} & a_{n-1\ 3} & \dots & a_{n-1\ n} & 0 \\ a_{n2} & a_{n3} & \dots & a_{nn} & 1 \end{vmatrix}.$$

Thus $\det M \cdot \det N =$

$$a_{11} \begin{vmatrix} a_{22} & a_{23} & \dots & a_{2\ n-1} \\ a_{32} & a_{33} & \dots & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 2} & a_{n-2\ 3} & \dots & a_{n-2\ n-1} \\ a_{n-1\ 2} & a_{n-1\ 3} & \dots & a_{n-1\ n-1} \end{vmatrix} |M_{11}| + \cdots - a_{n1} \begin{vmatrix} a_{22} & a_{23} & \dots & a_{2\ n-1} \\ a_{32} & a_{33} & \dots & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 2} & a_{n-2\ 3} & \dots & a_{n-2\ n-1} \\ a_{n-1\ 2} & a_{n-1\ 3} & \dots & a_{n-1\ n-1} \end{vmatrix} |M_{n1}|$$

$+L-L+K-K,$

where $L=$

$$-a_{12}\begin{vmatrix} a_{21} & a_{23} & \dots & a_{2\ n-1} \\ a_{31} & a_{33} & \dots & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 3} & \dots & a_{n-2\ n-1} \\ a_{n-1\ 1} & a_{n-1\ 3} & \dots & a_{n-1\ n-1} \end{vmatrix} |M_{11}| + \cdots + a_{1n-1} \begin{vmatrix} a_{21} & a_{22} & \dots & a_{2\ n-2} \\ a_{31} & a_{32} & \dots & a_{3\ n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 2} & \dots & a_{n-2\ n-2} \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-2} \end{vmatrix} |M_{11}|$$

and $K=$

$$a_{n2}\begin{vmatrix} a_{21} & a_{23} & \dots & a_{2\ n-1} \\ a_{31} & a_{33} & \dots & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 3} & \dots & a_{n-2\ n-1} \\ a_{n-1\ 1} & a_{n-1\ 3} & \dots & a_{n-1\ n-1} \end{vmatrix} |M_{n1}| + \cdots - a_{n\ n-1} \begin{vmatrix} a_{21} & a_{22} & \dots & a_{2\ n-2} \\ a_{31} & a_{32} & \dots & a_{3\ n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 2} & \dots & a_{n-2\ n-2} \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-2} \end{vmatrix} |M_{n1}|.$$

Thus

$$\det M \cdot \det N = |M_{nn}| \cdot |M_{11}| - |M_{1n}| \cdot |M_{n1}| + \Omega,$$

where $\Omega=$

$$\begin{vmatrix} a_{11} & 1 & 0 & \dots & 0 & 0 \\ a_{21} & 0 & a_{23} & \dots & a_{2\ n-1} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 1} & 0 & a_{n-1\ 3} & \dots & a_{n-1\ n-1} & 0 \\ a_{n1} & 0 & 0 & \dots & 0 & 1 \end{vmatrix} \begin{vmatrix} a_{12} & 0 & a_{13} & \dots & a_{1n} \\ a_{22} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 2} & a_{n-1\ 2} & a_{n-1\ 3} & \dots & a_{n-1\ n} \\ a_{n2} & 0 & a_{n3} & \dots & a_{nn} \end{vmatrix}$$

$+\cdots+$

$$\begin{vmatrix} a_{11} & 1 & 0 & \dots & 0 & 0 \\ a_{21} & 0 & a_{22} & \dots & a_{2\ n-2} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1\ 1} & 0 & a_{n-1\ 2} & \dots & a_{n-1\ n-2} & 0 \\ a_{n1} & 0 & 0 & \dots & 0 & 1 \end{vmatrix} \begin{vmatrix} a_{12} & \dots & a_{1\ n-1} & 0 & a_{1n} \\ a_{22} & \dots & a_{2\ n-1} & a_{2\ n-1} & a_{2n} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{n-1\ 2} & \dots & a_{n-1\ n-1} & a_{n-1\ n-1} & a_{n-1\ n} \\ a_{n2} & \dots & a_{n\ n-1} & 0 & a_{nn} \end{vmatrix}$$

$-L-K.$

Thus $\Omega =$

$$a_{n2}\begin{vmatrix} a_{21} & a_{23} & \dots & a_{2\ n-1} \\ a_{31} & a_{33} & \dots & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 3} & \dots & a_{n-2\ n-1} \\ a_{n-1\ 1} & a_{n-1\ 3} & \dots & a_{n-1\ n-1} \end{vmatrix} |M_{n1}| - a_{12} \begin{vmatrix} a_{21} & a_{23} & \dots & a_{2\ n-1} \\ a_{31} & a_{33} & \dots & a_{3\ n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 3} & \dots & a_{n-2\ n-1} \\ a_{n-1\ 1} & a_{n-1\ 3} & \dots & a_{n-1\ n-1} \end{vmatrix} |M_{11}|$$

$+ \cdots +$

$$a_{1\ n-1}\begin{vmatrix} a_{21} & a_{22} & \dots & a_{2\ n-2} \\ a_{31} & a_{32} & \dots & a_{3\ n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 2} & \dots & a_{n-2\ n-2} \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-2} \end{vmatrix} |M_{11}| - a_{n\ n-1} \begin{vmatrix} a_{21} & a_{22} & \dots & a_{2\ n-2} \\ a_{31} & a_{32} & \dots & a_{3\ n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2\ 1} & a_{n-2\ 2} & \dots & a_{n-2\ n-2} \\ a_{n-1\ 1} & a_{n-1\ 2} & \dots & a_{n-1\ n-2} \end{vmatrix} |M_{n1}|$$

$-L - K$

$= L + K - L - K = 0.$

In the same way we can do this when n is odd. □

Note that there are two other proofs of the above result. See Lemma 5.5 of [3] and Lemma 2.4 of [13] for details.

Corollary 2.3.6.

$$F_{n-2}^{q^2} F_n = F_{n-1}^q G_{n-1}, \quad n \geq 3.$$

Proof. This is proved by applying the above theorem to F_n and then using the fact that $G_{n-1} = F_{n-1}^{q^2-q+1} - F_{n-1}^{'}$. □

For the sake of convenience, we define $F_0 = 1$ so that the formula holds for $n = 2$.

Lemma 2.3.7. *(Lemma 1.4 in [14]).*

$$G_n^{'}(\xi_{n,0}, \xi_{n,1}, \dots, \xi_{n,n}) = 0.$$

Definition 2.3.8. Define the *weight* of the X_i as $\mathrm{wt}X_i = q^{2i+1} + 1$.

It is easy to verify that F_n, $F_n^{'}$, G_n and $G_n^{'}$ are all homogeneous with respect to their weights, and it is easy to see that

$$\mathrm{wt}G_n^{'} = \begin{cases} (q^{n+2}-1)(q^{n+1}+1)/(q^2-1), \text{if } n \text{ is even;} \\ (q^{n+1}-1)(q^{n+2}+1)/(q^2-1), \text{if } n \text{ is odd.} \end{cases}$$

Definition 2.3.9. Define the polynomial

$$Q_n^{'}(T) := G_n^{'}(X_0 - T^{q+1}, X_1 - T^{q^3+1}, \ldots, X_n - T^{q^{2n+1}+1})$$

where $Q_n^{'}(T) \in F_q[X_0, \ldots, X_n][T]$. This polynomial is designed so that

$$\begin{aligned} Q_{n-1}^{'}(\xi_{n,0}, \ldots, \xi_{n,n-1}, x_n) &= G_{n-1}^{'}(\xi_{n,0} - x_n^{q+1}, \ldots, \xi_{n,n-1} - x_n^{q^{2n-1}+1}) \\ &= G_{n-1}^{'}(\xi_{n-1,0}, \ldots, \xi_{n-1,n-1}). \end{aligned}$$

Thus, according to Lemma 2.3.7, we have

$$Q_{n-1}^{'}(\xi_{n,0}, \ldots, \xi_{n,n-1}, x_n) = G_{n-1}^{'}(\xi_{n-1,0}, \ldots, \xi_{n-1,n-1}) = 0.$$

Definition 2.3.10. Define the polynomials $P_n(T), P_n^{'}(T)$ and $Q_n(T)$ as follows:

$$P_n(T) := F_n(X_0 - T^{q+1}, X_1 - T^{q^3+1}, \ldots, X_{n-1} - T^{q^{2n-1}+1}),$$

$$P_n^{'}(T) := F_n^{'}(X_0 - T^{q+1}, X_1 - T^{q^3+1}, \ldots, X_n - T^{q^{2n+1}+1}),$$

$$Q_n(T) := G_n(X_0 - T^{q+1}, X_1 - T^{q^3+1}, \ldots, X_n - T^{q^{2n+1}+1}).$$

We now give the explicit form of $P_n(T)$ and $P_n^{'}(T)$ in the following theorem.

Theorem 2.3.11. *(Lemma 1.7 in [14]).*

(i) Let F_{ij} be the (i,j)-minor of the $n \times n$ matrix defining F_n, $1 \le i,j \le n$. Then

$$P_n(T) = F_n + \sum_{i,j=1}^{n} (-1)^{i+j+1} F_{ij} T^{q^{2i-1}+q^{2j-2}}.$$

(ii) Let $F_{ij}^{'}$ be the (i,j)-minor of the $n \times n$ matrix defining $F_n^{'}$, $1 \le i,j \le n$. Then

$$P_n^{'}(T) = F_n^{'} + \sum_{i,j=1}^{n} (-1)^{i+j+1} F_{ij}^{'} T^{q^{2i+1}+q^{2j-2}}.$$

In the following result we are going to define $R_{n,i}$ which has an important role in Theorem 2.3.17 and Theorem 2.3.18.

Proposition 2.3.12. *(Proposition 1.11 in [14]).*

(i) *Let* $\mathrm{wt}T = 1$, *then* $Q_n^{'}$ *is homogeneous and*

$$\mathrm{wt}Q_n^{'} = \begin{cases} (q^{n+2}-1)(q^{n+1}+1)/(q^2-1), & \text{if } n \text{ is even;} \\ (q^{n+1}-1)(q^{n+2}+1)/(q^2-1), & \text{if } n \text{ is odd.} \end{cases}$$

(ii) *Let* $Q_n^{'}(T) = \sum_{k=0}^{N} g_k(X_0, \ldots, X_n)T^k$, *then* $g_k(-H_{n-1,0}, \ldots, -H_{n-1,n}) = 0$ *for all* k.

(iii) *Let* $R_{n,i}$ *be the coefficient of* $T^{q^{2n+1-2i}+(-1)^n q^n}$ *in* $Q_n^{'}(T)$. *Then*

$R_{n,0} = (-1)^{n+1}G_{n-1}^{'}$ *is the leading coefficient of* $Q_n^{'}$;

$R_{n,i} = (-1)^n R_{n-2,i-1}^{q^2} X_n + f_{ni}(X_0, \ldots, X_{n-1})$, $1 \le i \le [\frac{n+1}{2}]$, $n \ge 2$;

$R_{1,0} = X_0$;

$R_{1,1} = X_0^{q^2-q+1} - X_1$;

$R_{2,0} = -X_0^{q^2-q+1} + X_1$;

$R_{2,1} = X_0^{\frac{q^5+1}{q+1}} - X_2 + G_1^{'} f_1(X_0, X_1)$.

(iv) *All the coefficients of* $Q_n^{'}$ *belong to the* $F_{q^2}[X_0, \ldots, X_{n-1}]$*-module generated by* $R_{n,0}, \ldots, R_{n,[(n+1)/2]}$.

Definition 2.3.13. Define a map Φ_n by the following rule:

$$\Phi_n : F_{q^2}[X_0, \ldots, X_{n-2}, Y_1, \ldots, Y_{[n/2]}] \to F_{q^2}\left[X_0, \ldots, X_{n-2}, \frac{R_{n-1,1}}{R_{n-1,0}}, \ldots, \frac{R_{n-1,[n/2]}}{R_{n-1,0}}\right]$$

$$X_i \to X_i, \quad Y_i \to \frac{R_{n-1,i}}{R_{n-1,0}}$$

Definition 2.3.14. Define A_m to be the $m \times (m+1)$ matrix

$$\begin{bmatrix}
g_{1,2m-2} & g_{1,2m-4}^{q^2} & g_{1,2m-6}^{q^4} & \cdots & \cdots & g_{12}^{q^{2m-4}} & f_{11}^{q^{2m-2}} & f_{10}^{q^{2m-2}} \\
g_{2,2m-2} & g_{2,2m-4}^{q^2} & g_{2,2m-6}^{q^4} & \cdots & g_{24}^{q^{2m-6}} & f_{23}^{q^{2m-4}} & f_{22}^{q^{2m-4}} & f_{21}^{q^{2m-4}} \\
\vdots & & & & & & & \vdots \\
g_{j,2m-2} & g_{j,2m-4}^{q^2} & \cdots & g_{j,2j}^{q^{2(m-j-1)}} & f_{j,2j-1}^{q^{2(m-j)}} & f_{j,2j-2}^{q^{2(m-j)}} & \cdots & f_{j,j-1}^{q^{2(m-j)}} \\
\vdots & & & & & & & \vdots \\
\vdots & & & & & & & \vdots \\
g_{m-1,2m-2} & f_{m-1,2m-3}^{q^2} & f_{m-1,2m-4}^{q^2} & \cdots & \cdots & \cdots & \cdots & f_{m-1,m-2}^{q^2} \\
f_{m,2m-1} & f_{m,2m-2} & f_{m,2m-3} & \cdots & \cdots & \cdots & \cdots & f_{m,m-1}
\end{bmatrix}$$

whose (i,j)th entry is

$$\begin{cases} g_{i,2(m-j)}^{q^{2j-2}}, & 1 \leq j \leq m-i; \\ f_{i,i-j+m}^{q^{2(m-i)}}, & m-i < j \leq m+1, \end{cases}$$

where $f_{ij} \in F_{q^2}[X_0, \ldots, X_j]$ and $g_{i,2j} \in F_{q^2}[X_0, \ldots, X_{2j}]$ are homogeneous polynomials.

Note the following simple observation about A_m: Define φ to be the operator which sends any polynomial to its q^2th power, and let φ operate on a matrix by operating on each of its entries. Then if we remove the first column and last row from A_m, the resulting $(m-1) \times m$ matrix is $\varphi(A_{m-1})$.

Definition 2.3.15. A ring R is a *unique factorization domain* (UFD) if it is a commutative domain and

(i) Every non-zero non-unit element $r \in R$ can be written as a product

$$r = x_1 \ldots x_n$$

of irreducibles in R; and

(ii) If r is a non-zero non-unit in R and

$$r = x_1 \ldots x_n = y_1 \ldots y_m,$$

where $x_1, \ldots, x_n, y_1, \ldots, y_m$ are irreducibles in R, then $n = m$ and, after re-ordering the y_j if necessary, x_i and y_i are associates for $i = 1, \ldots, n$.

Lemma 2.3.16. *$F[X_1, \ldots, X_n]$, where F is a field, is a unique factorization domain.*

Proof. Follows from Corollary 4 on page 295 in [17]. □

Theorem 2.3.17. *(Theorem E_n in [14]).*

(i) The kernel of the ring homomorphism Φ_{2n} in Definition 2.3.13 can be generated by $(n-1)$ polynomials $K_{2n,1}, \ldots, K_{2n,n-1}$ which have the following form:

$$\begin{bmatrix} K_{2n,1} \\ \vdots \\ K_{2n,n-1} \end{bmatrix} = \begin{bmatrix} g_{1,2n-2} \\ \vdots \\ g_{n-1,2n-2} \end{bmatrix} + \varphi(A_{n-1}) \begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix}.$$

(ii) The ring

$$\begin{aligned} &F_{q^2}\left[X_0, \ldots, X_{2n-2}, \frac{R_{2n-1,1}}{R_{2n-1,0}}, \ldots, \frac{R_{2n-1,n}}{R_{2n-1,0}}\right] \\ \cong\ &F_{q^2}[X_0, \ldots, X_{2n-2}, Y_1, \ldots, Y_n]/\langle K_{2n,1}, \ldots, K_{2n,n-1}\rangle \end{aligned}$$

is a UFD.

(iii) Let $R_{2n} \subseteq F_{q^2}[V]$ be the subring we get by substituting $H_{2n,i}$ for X_i in $F_{q^2}\left[X_0, \ldots, X_{2n-2}, \frac{R_{2n-1,1}}{R_{2n-1,0}}, \ldots, \frac{R_{2n-1,n}}{R_{2n-1,0}}\right]$, $0 \le i \le 2n-1$. Then $R_{2n} = F_{q^2}[V]^{U(2n,\ F_{q^2})}$.

Theorem 2.3.18. *(Theorem O_n in [14]).*

(i) The kernel of the ring homomorphism Φ_{2n+1} in Definition 2.3.13 can be generated by $(n-1)$ polynomials $K_{2n+1,1}, \ldots, K_{2n+1,n-1}$ which have the following form:

$$\begin{bmatrix} K_{2n+1,1} \\ \vdots \\ K_{2n+1,n-1} \end{bmatrix} = \begin{bmatrix} g_{1,2n-1} \\ \vdots \\ g_{n-1,2n-1} \end{bmatrix} + \varphi(B_{n-1}) \begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix}$$

where B_{n-1} is an $(n-1) \times n$ matrix whose (i,j)-entry is

$$\begin{cases} g_{i,2(n-j)-1}^{q^{2j-2}}, & 1 \le j \le n-i-1; \\ e_{i,i-j+n}^{q^{2(n-i-1)}}, & n-i-1 < j \le n. \end{cases}$$

Here $e_{ij} \in F_{q^2}[X_0, \ldots, X_j]$ and $g_{i,2j+1} \in F_{q^2}[X_0, \ldots, X_{2j+1}]$ are homogeneous polynomials.

(ii) The ring

$$F_{q^2}\left[X_0, \ldots, X_{2n-1}, \frac{R_{2n,1}}{R_{2n,0}}, \ldots, \frac{R_{2n,n}}{R_{2n,0}}\right]$$
$$\cong F_{q^2}[X_0, \ldots, X_{2n-1}, Y_1, \ldots, Y_n]/\langle K_{2n+1,1}, \ldots, K_{2n+1,n-1}\rangle$$

is a UFD.

(iii) Let $R_{2n+1} \subseteq F_{q^2}[V]$ be the subring we get by substituting $H_{2n+1,i}$ for X_i in $F_{q^2}\left[X_0, \ldots, X_{2n-1}, \frac{R_{2n,1}}{R_{2n,0}}, \ldots, \frac{R_{2n,n}}{R_{2n,0}}\right]$, $0 \leq i \leq 2n$. Then $R_{2n+1} = F_{q^2}[V]^{U(2n+1,\ F_{q^2})}$.

2.4 The invariant ring of the orthogonal group

Let $q = p^r$, p an odd prime, and suppose V is a vector space over F_q of dimension n with basis $e_1, \ldots, e_n$. Let $S = F_q[x_1, \ldots, x_n]$ where $x_1, \ldots, x_n$ is a basis of V^* dual to $e_1, \ldots, e_n$. It is known that all quadratic forms are equivalent to one of the following two quadratic forms:

$$Q_n^+ = x_1^2 - x_2^2 + x_3^2 - \cdots + (-1)^n x_{n-1}^2 + (-1)^{n+1} x_n^2, \quad n \geq 1;$$

$$Q_n^- = x_1^2 - \epsilon x_2^2 + \epsilon x_3^2 - \cdots + (-1)^n \epsilon x_{n-1}^2 + (-1)^{n-1} \epsilon x_n^2, \quad n \geq 1$$

where ϵ is a non-square in F_q^*. Let $O^+(n, F_q)$ be the orthogonal group associated with Q_n^+. In this section we describe the invariant rings of $O^+(n, F_q)$ for all n. Suppose

$$Q_n = \epsilon_1 x_1^2 + \epsilon_2 x_2^2 + \cdots + \epsilon_n x_n^2$$

where $\epsilon_i \in F_q^*$. Let $O(n, F_q)$ be the orthogonal group associated with Q_n. Suppose

$$Q_{n,i} = \epsilon_1 x_1^{q^i+1} + \epsilon_2 x_2^{q^i+1} + \cdots + \epsilon_n x_n^{q^i+1}$$

where $\epsilon_i \in F_q^*$. It is well known that

$$F_q(x_1, x_2, \ldots, x_n)^{O(n,\ F_q)} = F_q(Q_{n,0}, Q_{n,1}, \ldots, Q_{n,n-1})$$

as was calculated in [9].

Definition 2.4.1.

(i) The *Legendre symbol* is defined as follows:

$\left(\frac{\delta}{q}\right) = \delta^{\frac{q-1}{2}} = 1$, if δ is a square in F_q^*;

$\left(\frac{\delta}{q}\right) = \delta^{\frac{q-1}{2}} = -1$, if δ is a non-square in F_q^*.

(ii) Define the *weight* of the variables as follows:

$\mathrm{wt}x_i = \mathrm{wt}y_i = 1$ for all i; $\mathrm{wt}X_i = q^i + 1$, $\mathrm{wt}T = 1$.

Our aim is to construct two polynomials $g^{'+}$ and $g^{'-}$. For this consider the following matrix

$$M = \begin{bmatrix} X_0 & X_1 & X_2 & X_3 & X_4 & \cdots \\ X_1 & X_0^q & X_1^q & X_2^q & X_3^q & \cdots \\ X_2 & X_1^q & X_0^{q^2} & X_1^{q^2} & X_2^{q^2} & \cdots \\ X_3 & X_2^q & X_1^{q^2} & X_0^{q^3} & X_1^{q^3} & \cdots \\ X_4 & X_3^q & X_2^{q^2} & X_1^{q^3} & X_0^{q^4} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

whose (i,j)-entry is $X_{|j-i|}^{q^{min(i-1,j-1)}}$.

Suppose $M^{(n)}$ is the submatrix of the first n rows and n columns. Let $f_0 = 1$ and define $f_n = \det M^{(n)}$. Similarly let $f_0^{'} = 1$ and define $f_n^{'} = \det M_{1\ n+1}^{(n+1)}$. It is clear that $f_n \in F_q[X_0, X_1, \ldots, X_{n-1}]$ for $n \geq 1$ and $f_n^{'} \in F_q[X_0, X_1, \ldots, X_n]$ for $n \geq 1$. For example, $f_1 = X_0$, $f_2 = X_0^{q+1} - X_1^2$; $f_1^{'} = X_1$, $f_2^{'} = X_1^{q+1} - X_0^q X_2$. It is easy to show that

$$f_n = -f_{n-2}^q X_{n-1}^2 + \phi_1(X_0, X_1, \ldots, X_{n-1}), \quad \deg_{X_{n-1}} \phi_1 = 1 \ \ \forall\ n \geq 3;$$

$$f_n^{'} = (-1)^{n+1} f_{n-1}^q X_n + f_{n-2}^{'q} X_{n-1}^{q+1} + \phi_2(X_0, X_1, \ldots, X_{n-1}), \quad \deg_{X_{n-1}} \phi_2 = q \ \forall\ \ n \geq 3.$$

Definition 2.4.2.

$$g_n^+ = \begin{cases} f_n^{'} - f_n^{\frac{q+1}{2}}, & \text{for } n \equiv 0, 1 \pmod 4 \\ f_n^{'} + (-f_n)^{\frac{q+1}{2}}, & \text{for } n \equiv 2, 3 \pmod 4; \end{cases}$$

$$g_n^- = \begin{cases} f_n^{'} + f_n^{\frac{q+1}{2}}, & \text{for } n \equiv 0, 1 \pmod 4 \\ f_n^{'} - (-f_n)^{\frac{q+1}{2}}, & \text{for } n \equiv 2, 3 \pmod 4. \end{cases}$$

Definition 2.4.3. Let $g_{-1}^{'\pm} = 1$, $g_0^{'+} = X_0$, $g_0^{'-} = 1$ and define $g_n^{'\pm}$ as follows:

$$g_n^{'\pm} = g_n^{\pm}/(g_{n-2}^{'\mp})^q \quad \forall \quad n \geq 1.$$

Theorem 2.4.4. *(Lemma 2.5 in [13]).*

(i) $f_n = (-1)^{[\frac{n}{2}]} g_{n-1}^{'+} g_{n-1}^{'-}$,

(ii) $(g_{n-2}^{'\mp})^q | g_n^{\pm}$.

It is clear from the above theorem that $g_n^{'\pm}$ are polynomials.

Definition 2.4.5. Given $\epsilon \in F_q^*$, define the following polynomials:

$$F_{n,\epsilon}(X_0, \ldots, X_{n-1}; T) := f_n(X_0 + \epsilon T^2, X_1 + \epsilon T^{q+1}, \ldots, X_{n-1} + \epsilon T^{q^{n-1}+1})$$

$$F_{n,\epsilon}^{'}(X_0, \ldots, X_n; T) := f_n^{'}(X_0 + \epsilon T^2, X_1 + \epsilon T^{q+1}, \ldots, X_n + \epsilon T^{q^n+1})$$

$$G_{n,\epsilon}^{\pm}(X_0, \ldots, X_n; T) := g_n^{\pm}(X_0 + \epsilon T^2, X_1 + \epsilon T^{q+1}, \ldots, X_n + \epsilon T^{q^n+1})$$

$$G_{n,\epsilon}^{'\pm}(X_0, \ldots, X_n; T) := g_n^{'\pm}(X_0 + \epsilon T^2, X_1 + \epsilon T^{q+1}, \ldots, X_n + \epsilon T^{q^n+1}).$$

We now give the explicit form of $F_{n,\epsilon}(X_0, \ldots, X_{n-1}; T)$ and $F_{n,\epsilon}^{'}(X_0, \ldots, X_n; T)$ in the following theorem.

Theorem 2.4.6. *(Lemma 2.8 in [13]). Let f_{ij} and $f_{ij}^{'}$ be the (i,j)-minors of f_n and $f_n^{'}$, respectively, for $1 \leq i, j \leq n$. Then*

$$F_{n,\epsilon}(X_0, \ldots, X_{n-1}; T) = f_n + \sum_{i,j=1}^{n} (-1)^{i+j} \epsilon f_{ij} T^{q^{i-1}+q^{j-1}},$$

$$F_{n,\epsilon}^{'}(X_0, \ldots, X_n; T) = f_n^{'} + \sum_{i,j=1}^{n} (-1)^{i+j} \epsilon f_{ij}^{'} T^{q^{i}+q^{j-1}}.$$

We now describe the weights and T-degree of the polynomials defined in Definition 2.4.5.

Theorem 2.4.7. *(Lemma 2.9 in [13]). By using the definition of weight, we have that $F_{n,\epsilon}$, $F_{n,\epsilon}^{'}$, $G_{n,\epsilon}$, $G_{n,\epsilon}^{'}$ are homogeneous polynomials. The weights are as follows:*

(a) $\mathrm{wt}F_{n,\epsilon} = 2\left(\frac{q^n-1}{q-1}\right)$, $\mathrm{wt}F_{n,\epsilon}^{'} = (q+1)\left(\frac{q^n-1}{q-1}\right)$, $\mathrm{wt}G_{n,\epsilon}^{\pm} = (q+1)\left(\frac{q^n-1}{q-1}\right)$.

(b) If n is odd, then

$$\mathrm{wt}G'^{\pm}_{n,\epsilon} = \left(\frac{q^{n+1}-1}{q-1}\right).$$

(c) If n is even, then

$$\mathrm{wt}G'^{+}_{n,\epsilon} = (q^{\frac{n}{2}}+1)\left(\frac{q^{\frac{n}{2}+1}-1}{q-1}\right),$$

$$\mathrm{wt}G'^{-}_{n,\epsilon} = (q^{\frac{n}{2}+1}+1)\left(\frac{q^{\frac{n}{2}}-1}{q-1}\right).$$

Lemma 2.4.8. *(Lemma 2.10 in [13]). Consider the polynomials $F_{n,\epsilon}, F'_{n,\epsilon}, G^{\pm}_{n,\epsilon}$ and $G'^{\pm}_{n,\epsilon}$ as polynomials in T. Then*

(i) $\deg F_{n,\epsilon} = 2q^{n-1}, \quad \deg F'_{n,\epsilon} = q^{n-1}(q+1).$

(ii) $\deg G^{+}_{1,\epsilon} = q-(\frac{\epsilon}{q}),\ \deg G^{-}_{1,\epsilon} = q+(\frac{\epsilon}{q});\ \deg G^{+}_{n,\epsilon} = \deg G^{-}_{n,\epsilon} = q^{n-1}(q+1),\ n \geq 2.$

(iii) If n is even, then

$$\deg G'^{+}_{n,\epsilon} = q^n + q^{\frac{n}{2}}, \quad \deg G'^{-}_{n,\epsilon} = q^n - q^{\frac{n}{2}}.$$

(iv) If n is odd, then

$$\deg G'^{+}_{n,\epsilon} = q^n - (\tfrac{\epsilon}{q})q^{\frac{n-1}{2}}, \quad \deg G'^{-}_{n,\epsilon} = q^n + (\tfrac{\epsilon}{q})q^{\frac{n-1}{2}}.$$

Lemma 2.4.9. *(Lemma 2.12 in [13]). Let*

$$Q^{+}_{n,i} = x_1^{q^i+1} - x_2^{q^i+1} + x_3^{q^i+1} - \cdots + (-1)^n x_{n-1}^{q^i+1} + (-1)^{n+1} x_n^{q^i+1},\ n \geq 1$$

and

$$Q^{-}_{n,i} = x_1^{q^i+1} - \epsilon x_2^{q^i+1} + \epsilon x_3^{q^i+1} - \cdots + (-1)^n \epsilon x_{n-1}^{q^i+1} + (-1)^{n+1} \epsilon x_n^{q^i+1},\ n \geq 1$$

where ϵ is a non-square in F_q^*. Then

(i) $g'^{+}_n(Q^{+}_{n,0}, Q^{+}_{n,1}, \ldots, Q^{+}_{n,n}) = 0;$

(ii) $g'^{-}_n(Q^{-}_{n,0}, Q^{-}_{n,1}, \ldots, Q^{-}_{n,n}) = 0$ *for even* $n;$

(iii) $g'^{+}_n(Q^{-}_{n,0}, Q^{-}_{n,1}, \ldots, Q^{-}_{n,n}) = 0$ *for odd* $n.$

Theorem 2.4.10. *(i) For all $n \geq 1$, $G'^{+}_{n-1,\epsilon}(Q^+_{n,0}, Q^+_{n,1}, \ldots, Q^+_{n,n-1}; x_n) = 0$, where $\epsilon = (-1)^n$;*

(ii) For any positive even integer n, $G'^{+}_{n-1,\epsilon}(Q^-_{n,0}, Q^-_{n,1}, \ldots, Q^-_{n,n-1}; x_n) = 0$;

(iii) For any positive odd integer n, $G'^{-}_{n-1,-\epsilon}(Q^-_{n,0}, Q^-_{n,1}, \ldots, Q^-_{n,n-1}; x_n) = 0$.

Proof. (i) $G'^{+}_{n-1,\epsilon}(Q^+_{n,0}, Q^+_{n,1}, \ldots, Q^+_{n,n-1}; x_n)$

$= g'^{+}_{n-1}(Q^+_{n,0} + \epsilon x_n^2, Q^+_{n,1} + \epsilon x_n^{q+1}, \ldots, Q^+_{n,n-1} + \epsilon x_n^{q^{n-1}+1})$

$= g'^{+}_{n-1}(Q^+_{n-1,0}, Q^+_{n-1,1}, \ldots, Q^+_{n-1,n-1})$.

Thus by using the above lemma, we get

$$G'^{+}_{n-1,\epsilon}(Q^+_{n,0}, Q^+_{n,1}, \ldots, Q^+_{n,n-1}; x_n) = 0.$$

(ii) $G'^{+}_{n-1,\epsilon}(Q^-_{n,0}, Q^-_{n,1}, \ldots, Q^-_{n,n-1}; x_n)$

$= g'^{+}_{n-1}(Q^-_{n,0} + \epsilon x_n^2, Q^-_{n,1} + \epsilon x_n^{q+1}, \ldots, Q^-_{n,n-1} + \epsilon x_n^{q^{n-1}+1})$

$= g'^{+}_{n-1}(Q^-_{n-1,0}, Q^-_{n-1,1}, \ldots, Q^-_{n-1,n-1})$.

So by using the above lemma, we have

$$G'^{-}_{n-1,\epsilon}(Q^-_{n,0}, Q^-_{n,1}, \ldots, Q^-_{n,n-1}; x_n) = 0.$$

(iii) $G'^{-}_{n-1,-\epsilon}(Q^-_{n,0}, Q^-_{n,1}, \ldots, Q^-_{n,n-1}; x_n)$

$= g'^{-}_{n-1}(Q^-_{n,0} - \epsilon x_n^2, Q^-_{n,1} - \epsilon x_n^{q+1}, \ldots, Q^-_{n,n-1} - \epsilon x_n^{q^{n-1}+1})$

$= g'^{-}_{n-1}(Q^-_{n-1,0}, Q^-_{n-1,1}, \ldots, Q^-_{n-1,n-1})$.

Therefore by again using the above lemma, we have

$$G'^{-}_{n-1,-\epsilon}(Q^-_{n,0}, Q^-_{n,1}, \ldots, Q^-_{n,n-1}; x_n) = 0.$$

□

Definition 2.4.11. Define the polynomials $R^{\pm}_{n,i}(X_0, \ldots, X_n)$ in the following way.

(i) If n is even, the polynomial $G'^{+}_{n,-1}(X_0, X_1, \ldots, X_n; T)$ has degree $q^n + q^{\frac{n}{2}}$. Let $R^+_{n,i}$ be the coefficient of $T^{q^{n-i}+q^{\frac{n}{2}}}$, $i = 0, 1, \ldots, \frac{n}{2}$.

(ii) If n is odd and $\left(\frac{\epsilon}{q}\right) = 1$, the polynomial $G'^{+}_{n,\epsilon}(X_0, X_1, \ldots, X_n; T)$ has degree $q^n - q^{\frac{n-1}{2}}$. Let $R^{+}_{n,i}$ be the coefficient of $T^{q^{n-i}-q^{\frac{n-1}{2}}}$, $i = 0, 1, \ldots, \frac{n-1}{2}$; $R^{+}_{n,\frac{n+1}{2}}$ is the constant term.

(iii) If n is odd and $\left(\frac{\epsilon}{q}\right) = -1$, the polynomial $G'^{+}_{n,\epsilon}(X_0, X_1, \ldots, X_n; T)$ has degree $q^n + q^{\frac{n-1}{2}}$. Let $R^{-}_{n,i}$ be the coefficient of $T^{q^{n-i}+q^{\frac{n-1}{2}}}$, $i = 0, 1, \ldots, \frac{n+1}{2}$.

Definition 2.4.12. Define a $k \times (k+1)$ matrix A^k as

$$\begin{bmatrix} p_{1,2k-1} & p^{q}_{1,2k-3} & p^{q^2}_{1,2k-5} & \cdots & p^{q^{k-2}}_{13} & r^{q^{k-1}}_{12} & r^{q^{k-1}}_{11} \\ p_{2,2k-1} & p^{q}_{2,2k-3} & p^{q^2}_{2,2k-5} & \cdots & r^{q^{k-2}}_{24} & r^{q^{k-2}}_{23} & r^{q^{k-2}}_{22} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ r_{k,2k} & r_{k,2k-1} & r_{k,2k-2} & \cdots & r_{k,k+2} & r_{k,k+1} & r_{kk} \end{bmatrix}$$

whose (i,j)-entry is

$$\begin{cases} p^{q^{j-1}}_{i,2k-2j+1}, & \text{if } \ j \leq k-i; \\ r^{q^{k-i}}_{i,k+1+i-j}, & \text{if } \ j > k-i, \end{cases}$$

where p_{ij} and $r_{ij} \in F_q[X_0, X_1, \ldots, X_j]$.

Theorem 2.4.13. *(Theorem A_k in [13]). Let $n = 2k+1$ be a positive odd integer, $Q^{+}_{n} = x_1^2 - x_2^2 + x_3^2 - \cdots + x_{n-2}^2 - x_{n-1}^2 + x_n^2$ a quadratic form and let $O^{+}(n, F_q)$ be the orthogonal group associated to Q^{+}_{n}. Then*

(i) The invariant subring is

$$F_q[x_1, x_2, \ldots, x_n]^{O^{+}(n,\ F_q)}$$
$$= F_q\left[Q^{+}_{n,0}, Q^{+}_{n,1}, \ldots, Q^{+}_{n,n-2}, \frac{R^{+}_{n-1,1}(Q^{+}_{n,0}, \ldots, Q^{+}_{n,n-1})}{R^{+}_{n-1,0}(Q^{+}_{n,0}, \ldots, Q^{+}_{n,n-2})}, \ldots, \frac{R^{+}_{n-1,k}(Q^{+}_{n,0}, \ldots, Q^{+}_{n,n-1})}{R^{+}_{n-1,0}(Q^{+}_{n,0}, \ldots, Q^{+}_{n,n-2})}\right].$$

(ii) We have an isomorphism

$$\phi_n : F_q[X_0, X_1, \ldots, X_{n-2}, Y_1, Y_2, \ldots, Y_k]/\langle K_{n,1}, K_{n,2}, \ldots, K_{n,k-1}\rangle \rightarrow$$
$$F_q\left[X_0, X_1, \ldots, X_{n-2}, \frac{R^{+}_{n-1,1}(X_0, X_1, \ldots, X_{n-1})}{R^{+}_{n-1,0}(X_0, X_1, \ldots, X_{n-2})}, \ldots, \frac{R^{+}_{n-1,k}(X_0, X_1, \ldots, X_{n-1})}{R^{+}_{n-1,0}(X_0, X_1, \ldots, X_{n-2})}\right]$$

defined by

$$X_i \mapsto X_i \qquad (0 \leq i \leq n-2)$$

$$Y_j \mapsto \frac{R^+_{n-1,j}(X_0, X_1, \ldots, X_{n-1})}{R^+_{n-1,0}(X_0, X_1, \ldots, X_{n-2})} \quad (1 \leq j \leq k)$$

where the relations $K_{n,j}$ are defined by

$$\begin{bmatrix} K_{n,1} \\ K_{n,2} \\ \vdots \\ K_{n,k-1} \end{bmatrix} = A^k_{k;\emptyset} \begin{bmatrix} 1 \\ Y_1 \\ \vdots \\ Y_k \end{bmatrix}.$$

(iii) The polynomials p_{ij} and $r_{ij} \in F_q[X_0, X_1, \ldots, X_j]$ are independent of n and

$$r_{k,2k} = -X_{2k} + \psi(X_0, X_1, \ldots, X_{2k-1})$$

for some polynomial ψ.

Moreover, they are homogeneous with respect to the weight with

$$\begin{cases} \mathrm{wt} p_{ij} = q^{j+1} + q^{\frac{j+1}{2}-i}, & j \text{ odd}; \\ \mathrm{wt} r_{ij} = q^j + 1. \end{cases}$$

Theorem 2.4.14. *(Theorem C_k in [13]). Let $n = 2k$ be a positive even integer, $Q^+_n = x_1^2 - x_2^2 + x_3^2 - \cdots - x_{n-2}^2 + x_{n-1}^2 - x_n^2$ a quadratic form and let $O^+(n, F_q)$ be the orthogonal group associated to Q^+_n. Then*

(i) The invariant subring is

$$F_q[x_1, x_2, \ldots, x_n]^{O^+(n,\ F_q)}$$
$$= F_q\left[Q^+_{n,0}, Q^+_{n,1}, \ldots, Q^+_{n,n-2}, \frac{R^+_{n-1,1}(Q^+_{n,0}, \ldots, Q^+_{n,n-1})}{R^+_{n-1,0}(Q^+_{n,0}, \ldots, Q^+_{n,n-2})}, \ldots, \frac{R^+_{n-1,k}(Q^+_{n,0}, \ldots, Q^+_{n,n-1})}{R^+_{n-1,0}(Q^+_{n,0}, \ldots, Q^+_{n,n-2})}\right].$$

(ii) We have an isomorphism

$$\phi_n : F_q[X_0, X_1, \ldots, X_{n-2}, Y_1, Y_2, \ldots, Y_k]/\langle K_{n,1}, K_{n,2}, \ldots, K_{n,k-1}\rangle \to$$
$$F_q\left[X_0, X_1, \ldots, X_{n-2}, \frac{R^+_{n-1,1}(X_0, X_1, \ldots, X_{n-1})}{R^+_{n-1,0}(X_0, X_1, \ldots, X_{n-2})}, \ldots, \frac{R^+_{n-1,k}(X_0, X_1, \ldots, X_{n-1})}{R^+_{n-1,0}(X_0, X_1, \ldots, X_{n-2})}\right]$$

defined by

$$X_i \mapsto X_i \qquad (0 \leq i \leq n-2)$$

$$Y_j \mapsto \frac{R^+_{n-1,j}(X_0, X_1, \ldots, X_{n-1})}{R^+_{n-1,0}(X_0, X_1, \ldots, X_{n-2})} \quad (1 \leq j \leq k)$$

where the relations $K_{n,j}$ are defined by

$$\begin{bmatrix} K_{n,1} \\ K_{n,2} \\ \vdots \\ K_{n,k-1} \end{bmatrix} = C^k_{k;\emptyset} \begin{bmatrix} 1 \\ Y_1 \\ \vdots \\ Y_k \end{bmatrix}.$$

where

$$C^k = \begin{bmatrix} p'_{1,2k-2} & p'^{q}_{1,2k-4} & p'^{q^2}_{1,2k-6} & \cdots & p'^{q^{k-2}}_{12} & r'^{q^{k-1}}_{11} & r'^{q^{k-1}}_{10} \\ p'_{2,2k-2} & p'^{q}_{2,2k-4} & p'^{q^2}_{2,2k-6} & \cdots & r'^{q^{k-2}}_{23} & r'^{q^{k-2}}_{22} & r'^{q^{k-2}}_{21} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ r'_{k,2k-1} & r'_{k,2k-2} & r'_{k,2k-3} & \cdots & r'_{k,k+1} & r'_{k,k} & r'_{k,k-1} \end{bmatrix}$$

whose (i,j)th entry is

$$\begin{cases} p'^{q^{j-1}}_{i,2(k-j)}, & \text{if } j \leq k-i; \\ r'^{q^{k-i}}_{i,i-j+k}, & \text{if } j > k-i. \end{cases}$$

(iii) The polynomials p'_{ij} and $r'_{ij} \in F_q[X_0, X_1, \ldots, X_j]$ are independent of n and

$$r'_{k,2k-1} = -X_{2k-1} + \psi(X_0, X_1, \ldots, X_{2k-2})$$

for some polynomial ψ.

Moreover, they are homogeneous with respect to the weight with

$$\begin{cases} \mathrm{wt} p'_{ij} = q^{j+1} + q^{[\frac{j+1}{2}]-i}, & j \text{ even}; \\ \mathrm{wt} r'_{ij} = q^j + 1. \end{cases}$$

Chapter 3

Some properties of invariant rings

One of the main reasons we want to calculate generators of invariant rings and the relations among these generators is so that we can understand the structure of these rings. In this chapter we define Cohen-Macaulay, Gorenstein and graded complete intersection rings. We shall show that the information from Chapter 2 indicates that the invariant rings of symplectic, orthogonal (in the odd characteristic case) and unitary groups are Gorenstein and hence Cohen-Macaulay.

3.1 Projective and injective modules

In this section we define projective and injective modules. We give some examples of projective and injective modules. We also describe some properties of these.

Before introducing the concept of projective modules it is useful to define free modules.

Definition 3.1.1. Let R be a ring. For an R-module M the set $E \subseteq M$ is a basis for M if:

(i) E is a generating set for M;

(ii) E is linearly independent.

A free module is an R-module with a basis.

Example 3.1.2.

(i) Every vector space over a field F is free.

(ii) Let B be any non-trivial finite abelian group. Then B is not a free $\mathbb{Z}$-module. (For suppose B has a $\mathbb{Z}$-basis $\{f_1, \ldots, f_n\}$. Then $\exists\ m \in \mathbb{Z}, m \neq 0$ such that $f_1 m = f_1 m + f_2 0 + \cdots + f_n 0$ (take m to be the order of f_1).)

(iii) R^n is a free R-module.

Definition 3.1.3. Let R be a ring. An R-module M is *projective* if it is a direct summand of a free module.

Example 3.1.4.

(i) Any free module is projective.

(ii) If $e = e^2$ is a non-zero idempotent in R then eR is projective. (Since $R = eR \oplus (1-e)R$).

Let us state a result which gives equivalent conditions for projective modules.

Theorem 3.1.5. *The following conditions are equivalent for an R-module M.*

(i) M is projective.

(ii) The functor $Hom_R(M, \ )$ is exact. That is, the sequence

$$0 \to Hom(M, A) \to Hom(M, B) \to Hom(M, C) \to 0$$

is exact for every exact sequence

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

(iii) For every epimorphism $f : N \to N'$ and every module homomorphism $g : M \to N'$ there exists a homomorphism $h : M \to N$ such that $fh = g$.

Proof. Follows from the definition of projective module on page 33, Proposition 2.2.1 and Lemma 2.2.3 in [42]. □

Definition 3.1.6. Let R be a ring. An R-module J is called *injective* if and only if $\mathrm{Hom}_R(\quad, J)$ is an exact functor.

We now state a similar result to Theorem 3.1.5 but for injective modules.

Theorem 3.1.7. *The following are equivalent for an R-module J.*

(i) J is injective.

(ii) For any monomorphism $f : I \to I'$ and homomorphism $g : I \to J$ there exists a homomorphism $h : I' \to J$ such that $hf = g$.

Proof. Follows from Proposition 3.1.2 part (a) and (b) in [5]. □

We now consider $\mathbb{Z}$-modules and define divisible modules. See page 90 of [5].

Definition 3.1.8. Let A be a $\mathbb{Z}$-module. We say that A is *divisible* if and only if for all $a \in A$ and $0 \neq n \in \mathbb{Z}$ there exists $a' \in A$ with $na' = a$.

Lemma 3.1.9. *(Lemma 3.14 in [23]). Let J be a $\mathbb{Z}$-module. Then J is injective if and only if it is divisible.*

Example 3.1.10. *$\mathbb{Q}$ is injective as a $\mathbb{Z}$-module.*

3.2 Projective and injective resolution

In this section we define projective and injective resolutions. We give some examples of these.

Definition 3.2.1. Let R be a ring. Given an R-module M, a *projective resolution* of M is an exact sequence

$$\cdots \to P_n \to \cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

with all the P_i's projective.

Example 3.2.2. *Consider*

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \to 0$$

where $f(n) = 2n$ *and* $g(n) = n + 2\mathbb{Z}$. *This is a projective resolution of* $\mathbb{Z}/2\mathbb{Z}$.

Definition 3.2.3. Let R be a ring. Given an R-module M, an *injective resolution* of M is an exact sequence

$$0 \to M \to I_1 \to I_2 \to I_3 \to \cdots \to I_n \to \dots$$

with all the I_i's injective.

Example 3.2.4. *Consider*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Q} \xrightarrow{g} \mathbb{Q}/\mathbb{Z} \to 0$$

where $f(n) = n$ *and* $g(n) = n + \mathbb{Z}$. *This is an injective resolution of* $\mathbb{Z}$.

3.3 Ext functor

In this section our aim is to define Ext functor.

Before introducing the notion of Ext functor it is necessary to define chain complex and cochain complex. The following two definitions have been taken from [23].

Definition 3.3.1. Let R be a ring. A *chain complex* $(C_\bullet, d)$ of R-modules consists of a family $(C_n : \ n \in \mathbb{Z})$ of R-modules together with maps $d_n : C_n \to C_{n-1}$ for each $n \in \mathbb{Z}$ such that the composite of any two consecutive maps is zero, i.e.

$$d_{n-1}d_n = 0 \ \forall \ n \in \mathbb{Z}.$$

So a chain complex looks like this

$$\cdots \to C_{n+2} \xrightarrow{d_{n+2}} C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} C_{n-2} \to \dots$$

The nth *homology* $H_n(C_\bullet)$ is defined as.

$$H_n(C_\bullet) = \mathrm{Ker}d_n/\mathrm{Im}d_{n+1}.$$

Definition 3.3.2. Let R be a ring. A *cochain complex* $(C^\bullet, d)$ of R-modules consists of a family $(C^n : n \in \mathbb{Z})$ of R-modules together with maps $d^n : C^n \to C^{n+1}$ for each $n \in \mathbb{Z}$ such that the composite of any two consecutive maps is zero, i.e.

$$d^n d^{n-1} = 0 \ \forall \ n \in \mathbb{Z}.$$

So a cochain complex looks like this

$$\cdots \to C^{n-2} \xrightarrow{d^{n-2}} C^{n-1} \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^{n+1}} C^{n+2} \to \dots$$

The nth *cohomology* is defined as

$$H^n(C^\bullet) = \mathrm{Ker}d^n/\mathrm{Im}d^{n-1}.$$

Consider a chain complex of projective modules

$$\cdots \to P_j \to \cdots \to P_2 \to P_1 \to P_0 \to 0 \tag{3.1}$$

such that

$$\cdots \to P_j \to \cdots \to P_2 \to P_1 \to P_0 \to M \to 0 \tag{3.2}$$

is a projective resolution of a fixed module M. Let N be an R-module. By applying $\mathrm{Hom}_R(\ \ , N)$ to the chain complex in Equation (3.1) one gets a cochain complex as follows:

$$0 \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N) \to \mathrm{Hom}_R(P_2, N) \to \dots$$

$\mathrm{Ext}^n_R(M, N)$ is defined to be

$$\mathrm{Ext}^n_R(M, N) = H^n(\mathrm{Hom}_R(P_\bullet, N)).$$

Now since $P_1 \to P_0 \to M \to 0$ is exact, so

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N)$$

is exact. Therefore

$$\mathrm{Ker}(\mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N)) = \mathrm{Im}(\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N)).$$

It follows that

$$H^0(\mathrm{Hom}_R(P_\bullet, N)) = \mathrm{Im}(\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N)).$$

But $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N)$ is injective. Therefore, we get $\mathrm{Ext}^0_R(M, N) \cong \mathrm{Hom}_R(M, N)$.

3.4 Noetherian and Artinian modules

We defined unique factorization domains in chapter 2. This section is concerned with Noetherian and Artinian modules. We describe some properties of Noetherian modules. We also give some results on unique factorization domains which we shall use in chapter 5.

Definition 3.4.1. Let R be a ring. An R-module M in which all submodules are finitely generated is called *Noetherian*.

A ring R which is Noetherian as an R-module is called a Noetherian ring.

Definition 3.4.2. Let R be a ring. An R-module M which satisfies the descending chain condition with respect to inclusion is called Artinian.

A ring R which is Artinian as an R-module is called a Artinian ring.

Example 3.4.3.

(i) Fields and division rings are both Noetherian and Artinian.

(ii) $\mathbb{Z}$ is Noetherian.

Now let us state a well-known result called the Hilbert Basis Theorem.

Theorem 3.4.4. *If R is a Noetherian ring, then so is the polynomial ring $R[X]$.*

Proof. Follows from Theorem 3.3 of [30]. □

Corollary 3.4.5. *Let F be a field and $X_1, \ldots, X_n$ indeterminates. Then $F[X_1, \ldots, X_n]$ is a Noetherian ring.*

Proof. By induction on n from the above theorem. □

Lemma 3.4.6. *Let R be an integral domain. Then*

(i) Every prime element of R is irreducible.

(ii) If R is a UFD, every irreducible is prime.

It follows from above the lemma that prime and irreducible elements coincide in a UFD.

Proof. Follows from Theorem 2.5.2 in [38]. □

Our next result is based on localization. Thus before stating it we define localiztion. The following definition has been take from [30].

Definition 3.4.7. Let R be a ring. A subset S of R is called a multiplicative closed set if

(i) $1 \in S$,

(ii) $x, y \in S \implies xy \in S$.

Define a relation $\sim$ on $R \times S$ as follows:

$$(a, s) \sim (b, t) \text{ iff } (at - bs)u = 0 \text{ for some } u \in S.$$

It is easy to see that this is an equivalence relation. Let a/s denote the equivalence class of (a, s), and $S^{-1}R$ denote the set of equivalence classes. Sums and products are defined in $S^{-1}R$ as follows:

$$a/s + b/t = (at + bs)/st, \quad a/s \cdot b/t = ab/st.$$

This makes $S^{-1}R$ into a ring which is called the localization or ring of fractions. Now define a map $f : R \to S^{-1}R$ by $f(r) = r/1$. We see that f is a homomorphism. The kernel of this homomorphism is

$$\text{Ker} f = \{r \in R : rs = 0 \text{ for some } s \in S\}.$$

Hence f is injective if and only if S does not contain any zero-divisors of R. In particular, the set of all non-zero-divisors S of R is a multiplicative set; the ring fractions with respect to S is called total ring of fractions of R. If R is an integral domain then its total ring of fractions is the same as its field of fractions.

Note that if P is a prime ideal of R and $S = R - P$ then we denote the localization by R_P.

Lemma 3.4.8. *(Lemma 6.3.1 in [4]). Suppose that R is a Noetherian integral domain. If $x \in R$ is a prime and $R[x^{-1}]$ is a unique factorization domain, then R is also a unique factorization domain.*

3.5 Dimension and height

In this section we define minimal prime ideals over any ideal I. We also define equidimensional rings, height and dimension. We show that any polynomial ring over a field is an equidimensional ring. We give two proofs. For this we have taken some results from [22], [31] and [37]. The others results which have been taken from [2] and [29] as well as some of the result from [22] and [37] will be used in later sections.

Definition 3.5.1. Let R be a ring. The supremum of the lengths r, taken over all strictly decreasing chains $P_0 \supset P_1 \supset \cdots \supset P_r$ of prime ideals of R, is called the *Krull dimension*, or simply the *dimension* of R, and denoted as $\dim R$.

Example 3.5.2.

(i) $\dim F = 0$, *where F is any field.*

(ii) $\dim \mathbb{Z} = 1$.

If M is an R-module, we define the dimension of M by $\dim M = \dim(R/\mathrm{ann}(M))$ where

$$\mathrm{ann}(M) = \{a \in R : am = 0 \ \forall \ m \ \in M\}.$$

Lemma 3.5.3. *(Corollary of Theorem 5.6 in [30]).* $\dim(F[X_1, \ldots, X_n]) = n$, *where F is any field.*

Definition 3.5.4. Let R be a ring. For a prime ideal P of R, the supremum of the lengths, taken over all strictly decreasing chains of prime ideals $P = P_0 \supset P_1 \supset \cdots \supset P_r$ starting from P, is called the *height* of P, and denoted by $\mathrm{ht}P$.

It follows from this definition that $\mathrm{ht}P = \dim R_P$ and $\mathrm{ht}P + \dim(R/P) \leq \dim R$.

What happens if P is not a prime ideal?

Definition 3.5.5. For an ideal I of a ring R, we define the height of I to be

$\mathrm{ht}I = \inf\{\mathrm{ht}P : I \subset P \in \mathrm{Spec}R\}$.

It follows that

$\mathrm{ht}I + \dim(R/I) \leq \dim R$.

Lemma 3.5.6. *(Theorem 47 in [29]). A Noetherian integral domain is a UFD if and only if every height 1 prime ideal is principal.*

We now present a nice result which gives a relation between height and dimension.

Proposition 3.5.7. *(Proposition 15 on page 45 in [37]). Let R be a domain which is a finitely generated algebra over a field F and $n = \dim R$. For every prime ideal P of R, we have*

$$\mathrm{ht}P + \dim(R/P) = n.$$

Definition 3.5.8. A prime ideal P in a ring R is said to be *minimal* over an ideal I if there are no prime ideals strictly contained in P that contain I. A prime ideal is said to be a minimal prime ideal if it is a minimal prime ideal over the zero ideal.

Let us state some properties.

Lemma 3.5.9. *Let R be a Noetherian ring and I an ideal in R. Then there are only a finite number of prime ideals minimal over I.*

Proof. Follows from Theorem 88 in [22]. □

Theorem 3.5.10. *(Corollary 11.17 in [2]). Let R be a Noetherian ring and let x be an element of R which is neither a zero-divisor nor a unit. Then every minimal prime ideal P over $\langle x \rangle$ has height 1.*

The above theorem is called Krull's principal ideal theorem.

We now state some results which will help us to show that every maximal ideal in $F[X_1, \ldots, X_n]$ has height n.

Lemma 3.5.11. *(Corollary 2 on page 44 in [37]). Let R be a finitely generated algebra over a field F, and let m be a maximal ideal of R. Then R/m is a finite extension of F.*

Lemma 3.5.12. *(Lemma 1.26 in [31]). Let R be an integral domain that contains a field as a subring. If R is a finite dimensional when viewed as a vector space over F. Then R is a field.*

Lemma 3.5.13. *(Theorem 149 in [22]). Let R be a Noetherian ring and P a prime ideal in R with $htP = n$. Denote by $P^* = PR[X]$ the expansion of P to $R[X]$, and let $Q \neq P^*$ be a prime ideal in $R[X]$ with $Q \cap R = P$. Then $htP^* = n$ and $htQ = n+1$.*

We are now going to prove that every maximal ideal in $F[X_1, \ldots, X_n]$ has height n. The idea comes from page 109 of [22].

Suppose F is a field and $R = F[X_1, \ldots, X_n]$. Let J be a maximal ideal in R and $S = F[X_1, \ldots, X_{n-1}]$. Set $I = J \cap S$. Then

$$S/I = S/(J \cap S) \cong (S + J)/J \subseteq R/J.$$

By Lemma 3.5.11 R/J is a finite field extension of F, therefore $\dim_F(R/J) < \infty$. Now since

$$F \subseteq S/I \subseteq R/J$$

it follows that $\dim_F(S/I) < \infty$ and S/I is an integral domain. Therefore by Lemma 3.5.12 S/I is a field and so I is a maximal ideal in S. Now we claim that $IR \subsetneq J$. Define a map θ as follows:

$$\theta : R \to (S/I)[X_n]$$

$$\sum_{\alpha} \lambda_\alpha X_1^{\alpha_1} \ldots X_n^{\alpha_n} \mapsto \sum_{\alpha} \bar{\lambda}_\alpha \bar{X}_1^{\alpha_1} \ldots \bar{X}_{n-1}^{\alpha_{n-1}} X_n^{\alpha_n}.$$

It is an epimorphism and $\mathrm{Ker}\theta = I[X_n]$. It is easy to see that $I[X_n] = IR$ so we get $R/IR \cong (S/I)[X_n]$. Since $(S/I)[X_n]$ is a polynomial ring therefore $IR \subsetneq J$. By induction, we may assume $\mathrm{ht}I = n - 1$. By the above lemma, $\mathrm{ht}J = n$.

Definition 3.5.14. A ring R is *equidimensional* if all maximal ideals have the same height.

From our above discussion it is clear that $F[X_1, \ldots, X_n]$ is an equidimensional ring. We are now going to define saturated and maximal chains. The following definition has been taken from [37].

Definition 3.5.15. A chain of prime ideals is called *saturated* if it is not contained in any other chain with the same origin and extremity (in other words, if one cannot interpolate any prime ideal between the elements of the chain). It is called *maximal* if it is saturated, its origin is a minimal prime ideal, and its extremity is a maximal ideal.

Notice that it can also be shown in the following way that $F[X_1, \ldots, X_n]$ is an equidimensional ring. The idea comes from the proof of Corollary 2 of Proposition 15 on page 45 in [37]. Let $R = F[X_1, \ldots, X_n]$ and P_l be a maximal ideal in R. Consider a maximal chain of prime ideals

$$P_l \supset \cdots \supset P_0.$$

Since it is maximal, we have $P_0 = 0$. We therefore have

$$\dim(R/P_0) = \dim R \text{ and } \dim(R/P_l) = 0.$$

Moreover, since the chain is saturated, one cannot interpolate any prime ideal between P_i and P_{i-1}; thus $\mathrm{ht}(P_i/Pi - 1) = 1$ and so by Proposition 3.5.7 we have

$$\dim(R/P_{i-1}) - \dim(R/P_i) = 1.$$

As $\dim(R/P_0) = \dim R$ and $\dim(R/P_l) = 0$, we deduce that $l = \dim R$. Thus it follows that $\mathrm{ht} P_l = \dim R$. Therefore every maximal ideal in R has the same height which is $\dim R$.

Lemma 3.5.16. *(Theorem 155 in [22]). Let P be a prime ideal in a Noetherian ring R and let x be an element in P. Suppose the height of P in R is k. Then the height of $P/\langle x\rangle$ in $R/\langle x\rangle$ is k or $k-1$. If x is not contained in any minimal prime*

ideal of R (and so, in particular if x is a non-zero divisor) then the height of $P/\langle x\rangle$ in $R/\langle x\rangle$ is $k-1$.

See Remark 3.6.12 for further details.

Lemma 3.5.17. *Let R be a finitely generated graded commutative algebra over a field F of Krull dimension d and $a_1,\ldots,a_j$ elements of R. Then* $\dim(R/\langle a_1,\ldots,a_j\rangle) \geq d-j$.

Proof. Follows from Proposition 5.3.10 in [39]. □

It should be noted that a similar result holds when we consider R to be a local ring with a maximal ideal m. In this case $a_1,\ldots,a_j \in m$. See Corollary 10.9 in [18] for further details.

3.6 Regular sequences, Depth and grade

In this section we define regular sequences, depth and grade. We give some useful results on these. These results have been taken from [13] and [30].

Definition 3.6.1. Let R be a ring and M an R-module. An element $a \in R$ is said to be *M-regular* if $ax \neq 0$ for all $0 \neq x \in M$. A sequence $a_1,\ldots,a_n$ of elements of R is an *M-sequence* (or an *M-regular sequence*) if the following conditions hold:

(i) a_1 is M-regular, a_2 is (M/a_1M)-regular,..., a_n is $(M/(a_1M+\cdots+a_{n-1}M))$-regular;

(ii) $M/\sum_{i=1}^{n} a_iM \neq 0$.

Example 3.6.2.

(i) Let R be a ring and $S = R[X_1,\ldots,X_n]$. Then $X_1,\ldots,X_n$ is an S-regular sequence.

(ii) Let F be a field and $A = F[X,Y,Z]$. Set $a_1 = X(Y-1)$, $a_2 = Y$ and $a_3 = Z(Y-1)$, then a_1,a_2,a_3 is a regular sequence but a_1,a_3,a_2 is not.

Thus it follows from the above example that a permutation of a regular sequence need not be a regular sequence.

We are now going to state some results on regular sequences which will be used in chapter 5.

Theorem 3.6.3. *(Theorem 16.1 in [30]). Let M be an R-module and $a_1, \ldots, a_n \in R$. If $a_1, \ldots, a_n$ is an M-sequence then so is $a_1^{v_1}, \ldots, a_n^{v_n}$ for positive integers $v_1, \ldots, v_n$.*

The following two results have been taken from [13] in which $R = R_1 \oplus R_2 \oplus \ldots$ is a positively graded ring.

Lemma 3.6.4. *(Lemma 3.15 in [13]). Let $x_1, \ldots, x_n \in R$ be homogeneous elements of positive degrees. If $x_1, \ldots, x_n$ is a regular sequence, then $x_1, \ldots, x_n$ is a regular sequence in any order.*

Lemma 3.6.5. *(Lemma 3.17 in [13]). For any $x \in R$, we denote its homogeneous component of the highest degree by $in(x)$. Suppose $x_1, \ldots, x_n \in R$, not necessarily homogeneous. If $in(x_1), \ldots, in(x_n)$ is a regular sequence, then $x_1, \ldots, x_n$ is a regular sequence.*

Lemma 3.6.6. *(Lemma 3.13 part (a) in [13]). Let R be a ring. If $x_1, \ldots, x_i \ldots, x_n$ and $x_1, \ldots, x_{i-1}, x_i^{'}, x_{i+1}, \ldots, x_n \in R$ are regular sequences. Then*

$$x_1, \ldots, x_{i-1}, x_i x_i^{'}, x_{i+1}, \ldots, x_n \in R$$

is a regular sequence.

Definition 3.6.7. Let R be a ring. The *depth* of an R-module M is the length of the longest regular sequence for M. The depth of the ring R is its depth as an R-module.

Example 3.6.8. *Let F be a field.*

(i) $\text{depth}F = 0$.

(ii) $\text{depth}F[X_1, \ldots, X_n] = n$.

The following two definitions have been taken from [28].

Definition 3.6.9. Let R be a Noetherian ring. We define the *grade* of an ideal I to be the maximal length of an R-sequence in I on R and denote it $\mathrm{G}_R(I)$. Similarly for an R-module M we define $\mathrm{G}_R(I, M)$ to be the length of a maximal R-sequence in I on M.

Definition 3.6.10. Let R be a ring and M an R-module. Define

$$r(M) := \inf\{i : \mathrm{Ext}^i(M, R) \neq 0\}.$$

We now describe an important result which will be used in later sections.

Proposition 3.6.11. *Let R be a Noetherian ring. Then $G(I) = r(R/I)$ for every ideal I of R.*

Proof. Follows from Theorem 16.7 in [30]. □

Remark 3.6.12. Note that in Lemma 3.5.16 if $x_1, \ldots, x_t \in P$ is a regular sequence in R then it follows by induction on n that the height of $P/\langle x_1, \ldots, x_t\rangle$ in $R/\langle x_1, \ldots, x_t\rangle$ is $k - t$.

3.7 Cohen-Macaulay and Gorenstein Rings

In this section we define Cohen-Macaulay and Gorenstein rings. We give some results related to Cohen-Macaulay and Gorenstein rings which are useful here. The results have been taken from different sources: [4], [5], [22], [28], [30] and [37]. At the heart of this section we prove some results which are old but which we do not have specific references for. We shall use these results in the last section.

Definition 3.7.1. Suppose that R is a Noetherian local ring and let M be a finitely generated R-module. We say that M is a *Cohen-Macaulay* module (CM-module) if $M \neq 0$ and $\mathrm{depth}M = \dim M$. If R itself is a CM-module, we say that R is a CM ring or Macaulay ring.

What happens if R is not local?

Definition 3.7.2. A Noetherian ring R is said to be a CM ring if R_m is a CM local ring for every maximal ideal m of R.

Example 3.7.3. *Let F be a field.*

(i) The ring $F[X_1, \ldots, X_n]$ is Cohen-Macaulay.

(ii) The ring $F[X^4, X^3Y, XY^3, Y^4] \subset F[X, Y]$ is not Cohen-Macaulay.

We now present some properties of Cohen-Macaulay rings.

Theorem 3.7.4. *(Theorem 151 in [22]). Let R be a ring. Then R is a CM ring if and only if $R[X]$ is a CM ring.*

Corollary 3.7.5. *Let R be a ring. Then R is a CM ring if and only if $R[X_1, \ldots, X_n]$ is a CM ring.*

Proof. By induction on n from the above theorem. □

Theorem 3.7.6. *(Theorem 141 in [22]). Suppose that R is a Cohen-Macaulay ring and $x \in R$ is not a zero-divisor. Then $R^* = R/\langle x \rangle$ is a Cohen-Macaulay ring.*

Corollary 3.7.7. *Let $x_1, \ldots, x_n$ be a regular sequence in a Cohen-Macaulay ring R. Then $R^* = R/\langle x_1, \ldots, x_n \rangle$ is a Cohen-Macaulay ring.*

Proof. By induction on n from the above theorem. □

Lemma 3.7.8. *(Theorem 1.1.11 in [28]). Let R be an equidimensional Cohen-Macaulay ring. Then for any finitely generated module M*

$$\dim R = \dim M + r(M).$$

Lemma 3.7.9. *(Theorem 136 in [22]). Grade and height coincide for every ideal in a Cohen-Macaulay ring.*

Theorem 3.7.10. *Let R be an equidimensional Cohen-Macaulay ring. Then for any ideal I*

$$\dim R = \dim(R/I) + \mathrm{ht} I.$$

Proof. From Lemma 3.7.8, we have $\dim R = \dim(R/I)+r(R/I)$. But by Proposition 3.6.11, we have $\mathrm{G}(I) = r(R/I)$. Therefore $\dim R = \dim(R/I)+\mathrm{G}(I)$. Now by Lemma 3.7.9, we have $\mathrm{G}(I) = \mathrm{ht}I$. Thus $\dim R = \dim(R/I)+\mathrm{ht}I$. □

Corollary 3.7.11. *Let R be an equidimensional Cohen-Macaulay ring. Suppose x is an element of R which is neither a zero-divisor nor a unit. Then*

$$\dim(R/\langle x\rangle) = \dim R - 1.$$

Proof. By the above theorem, we have $\dim R = \dim(R/\langle x\rangle)+\mathrm{ht}\langle x\rangle$ but according to Theorem 3.5.10 we have $\mathrm{ht}\langle x\rangle = 1$. Therefore we have $\dim(R/\langle x\rangle) = \dim R - 1$. □

Corollary 3.7.12. *Let R be an equidimensional Cohen-Macaulay ring. Suppose $x_1, \ldots x_r$ is a regular sequence in R. Then*

$$\dim(R/\langle x_1, \ldots, x_r\rangle) = \dim R - r.$$

Proof. By induction on n from the above corollary. □

It follows from page 3 of [28] that a local ring is equidimensional. Thus Theorem 3.7.10, Corollary 3.7.11 and Corollary 3.7.12 are still true when R is a Cohen-Macaulay local ring. Now we are going to state a similar result to Corollary 3.7.12 which gives an equivalent condition for Cohen-Macaulay rings. We shall use this result in chapter 5.

Theorem 3.7.13. *(Proposition 4.3.4 in [4]). Let R be a Noetherian ring and M a finitely generated R-module. Suppose that one of the following conditions hold.*

(i) R is local, with maximal ideal m, so that $F = R/m$ is a field, or

(ii) $R = \bigoplus_{j=0}^{\infty} R_j$ and $M = \bigoplus_{j=-\infty}^{\infty} M_j$ are graded, with $R_0 = F$ a field, and R is finitely generated over F by elements of positive degree. In this case, we write m for the ideal R^+ generated by the elements of positive degree.

If M is Cohen-Macaulay then a sequence $x_1, \ldots, x_r$ is regular for M if and only if

$$\dim(M/(x_1M + \cdots + x_rM)) = \dim M - r.$$

Let us state a similar result to Theorem 3.7.10. Here instead of an equidimensional Cohen-Macaulay ring we consider a Cohen-Macaulay local ring.

Lemma 3.7.14. *Let (R, m) be a Cohen-Macaulay local ring. For a proper ideal I of R we have*

$$\mathrm{ht}I + \dim(R/I) = \dim R.$$

Proof. Follows from Theorem 17.4 in [30]. □

Lemma 3.7.15. *(Corollary 3 on page 67 in [37]) Let R be a local ring which is a quotient of a Cohen-Macaulay ring. Let $P' \supset P$ be two prime ideals of R. Then all saturated chains of prime ideals joining P' to P have the same length, which is* $\dim(R/P) - \dim(R/P')$.

It follows from the above lemma that if R is a Cohen-Macaulay local ring, then every maximal chain of prime ideals in R has the same length which is $\dim R$.

Theorem 3.7.16. *Suppose $R = F[X_1, \ldots, X_n]$ and that $S = R/I$, where $I = \sum_{i=1}^{t} R\rho_i$ and $\{\rho_1, \ldots, \rho_t\}$ is a regular sequence. Then all maximal chains of prime ideals in S have the same length which is* $\dim S$.

Proof. Let $\bar{m} = m/I$ be a maximal ideal of S. Consider the localization $S_{\bar{m}}$. Let

$$\bar{m}S_{\bar{m}} \supset \bar{P}_r S_{\bar{m}} \supset \bar{P}_{r-1} S_{\bar{m}} \supset \cdots \supset \bar{P}_1 S_{\bar{m}} \tag{3.3}$$

be a maximal chain of prime ideals in $S_{\bar{m}}$. According to the above lemma the length of this chain is

$\dim(S_{\bar{m}}/\bar{P}_1 S_{\bar{m}}) - \dim(S_{\bar{m}}/\bar{m}S_{\bar{m}}) = \dim(S_{\bar{m}}/\bar{P}_1 S_{\bar{m}})$.

By Lemma 3.7.14 we have

$\dim(S_{\bar{m}}/\bar{P}_1 S_{\bar{m}}) = \dim S_{\bar{m}} = \mathrm{ht}\bar{m}$.

Now by the Correspondence Theorem m is a maximal ideal of R and we know that R is equidimensional. Thus $\mathrm{ht}m = n$ and so by Remark 3.6.12 $\mathrm{ht}\bar{m} = n - t$. From Corollary 3.7.12 $\dim S = n - t$. Thus every maximal chain of prime ideals in $S_{\bar{m}}$ has the same length which is $\dim S$. Now from Equation (3.3) we get the following strict chain:

$$\bar{m}S_{\bar{m}} \cap S \supset \bar{P}_r S_{\bar{m}} \cap S \supset \bar{P}_{r-1} S_{\bar{m}} \cap S \supset \cdots \supset \bar{P}_1 S_{\bar{m}} \cap S.$$

Since $\bar{m}S_{\bar{m}} \cap S = \bar{m}$ and $\bar{P}_i S_{\bar{m}} \cap S = \bar{P}_i$ so we get the strict chain

$$\bar{m} \supset \bar{P}_r \supset \bar{P}_{r-1} \supset \cdots \supset \bar{P}_1$$

which has the same length as the length of the chain in Equation (3.3). This completes the proof. □

Note that a similar result holds if S is an integral domain which is a finitely generated algebra. See Corollary 2 of Proposition 15 on page 45 in [37] for details.

A multiplicativey closed set S is said to be saturated if every divisor of $x \in S$ is in S. Following Kaplansky, we note that if M is a non-zero R-module and

$$S = \{x \in R : mx \neq 0 \ \forall \ 0 \neq m \in M\}$$

then S is a saturated multiplicatively closed set and $R \setminus S$ is a set-theoretic union of prime ideals. The prime ideals maximal among these may be called the maximal primes of zero-divisors of M.

Definition 3.7.17. Let R be a ring, M any non-zero R-module. The prime ideals contained in and maximal within the zero-divisors of M are called *maximal primes* of M. When M has the form R/I, I an ideal of R, we use the terminology *maximal primes belonging* to I, rather than *of* R/I.

Lemma 3.7.18. *(Theorem 137 in [22]). In a Cohen-Macaulay ring R let I be an ideal of height n, which can be generated by n elements. Then all maximal primes belonging to I have height n and are minimal over I.*

Definition 3.7.19. Let (R, m, F) be an n-dimensional Noetherian local ring with maximal ideal m and $F = R/m$. Then R is said to be a *Gorenstein ring* if any of the following equivalent conditions hold.

(i) $\mathrm{Ext}^i_R(F, R) = 0$ for $i \neq n$ and $\mathrm{Ext}^i_R(F, R) \cong F$ for $i = n$.

(ii) $\mathrm{Ext}^i_R(F, R) = 0$ for some $i > n$.

(iii) $\mathrm{Ext}^i_R(F, R) = 0$ for $i < n$ and $\mathrm{Ext}^i_R(F, R) \cong F$ for $i = n$.

(iv) R is a CM ring and $\mathrm{Ext}^n_R(F, R) \cong F$.

Note that the equivalence of the above conditions follows from Theorem 18.1 in [30]. Again what happens if R is not local?

Definition 3.7.20. A Noetherian ring R is Gorenstein if its localization at every maximal ideal is a Gorenstein local ring.

It is very clear from the definition that every Gorenstein ring is CM. Let us now describe some properties of Gorenstein rings.

Theorem 3.7.21. *If R is Gorenstein then so is the polynomial ring $R[X]$.*

Proof. This is exercise 18.3 in [30] and the solution is on page 294. □

Corollary 3.7.22. *If R is Gorenstein then so is the polynomial ring $R[X_1, \ldots, X_n]$.*

Proof. By induction on n from the above theorem. □

Theorem 3.7.23. *(Theorem 221 in [22]). Let R be a zero-dimensional local ring with maximal ideal m. Then R is Gorenstein if and only if the annihilator of m is one dimensional (as a vector space over R/m).*

Example 3.7.24.

(i) The ring $F[X_1, \ldots, X_n]$ is Gorenstein.

(ii) Let $S = F[X, Y]/\langle X^2, XY, Y^2\rangle$, then S is CM but not Gorenstein.

Solution:

(i) Follows from Corollary 3.7.22.

(ii) Let $m = \langle X, Y\rangle/\langle X^2, XY, Y^2\rangle$ which is a maximal ideal in S. Since $m^2 = 0$ S is a local ring with maximal ideal m. Now $\dim_F S = 3$ therefore S is both Noetherian and Artinian. Since S is Artinian $\dim S = 0$ and so S is CM. Now $\mathrm{ann}(m) = m$ and $\dim_F(\mathrm{ann}(m)) = 2$. Thus according to Theorem 3.7.23 S is not Gorenstein.

Theorem 3.7.25. *If R is Gorenstein and $x_1, \ldots, x_n$ is a regular sequence in R, then $R/\langle x_1, \ldots, x_n\rangle$ is Gorenstein.*

Proof. Follows from Proposition 3.1.19 part (b) in [5]. □

3.8 Graded complete intersection

In this section we define graded complete intersections. We prove a useful result which gives an equivalent condition for graded complete intersections. We show that the calculations in [8], [13] and [14] indicate that the invariant rings of symplectic, orthogonal (in the odd characteristic case) and unitary groups are Gorenstein.

Definition 3.8.1. A finitely generated graded algebra R is said be a *graded complete intersection* if the minimal number of generators minus the minimal number of generating relations between them is equal to the Krull dimension $\dim R$.

Theorem 3.8.2. *A finitely generated graded algebra is a graded complete intersection if and only if the relations in the generators form a regular sequence.*

Proof. Suppose $R = F[X_1, \ldots, X_n]$ and that $S = R/I$, where $I = \sum_{i=1}^{t} R\rho_i$ and $\{\rho_1, \ldots, \rho_t\}$ is a regular sequence. We claim that it is a graded complete intersection. By Corollary 3.7.12 we have $\dim S = n-t$. Next we need to show that t is the minimal number of generators of I. Suppose I can be generated by w elements with $w < t$. Then $\dim S = \dim(R/I) \geq n-w$ by Lemma 3.5.17 and $n-w > n-t = \dim S$. Thus we get a contradiction.

Conversely suppose $S = R/J$, $R = F[X_1, \ldots, X_n]$ where J has minimal generating set $\{z_1, \ldots, z_r\}$ and $\dim S = n-r$. We claim that $\{z_1, \ldots, z_r\}$ is an R- sequence. Suppose that $\{z_1, \ldots, z_i\}$ is an R-sequence, where $0 \leq i < r$; we need to show that z_{i+1} is not a zero-divisor modulo $\sum_{j=1}^{i} Rz_j$. Let $I = \sum_{j=1}^{i} Rz_j$ and $\bar{R} = R/I$. Now R is an equidimensional Cohen-Macaulay ring so by Theorem 3.7.10 $\mathrm{ht} I = i$. Thus by Lemma 3.7.18, the set of zero divisors of $\bar{R}$ is $\bigcup_{\lambda\in\Lambda} P_\lambda$ where P_λ are minimal prime ideals of $\bar{R}$. Now $\bar{R}$ is Noetherian so by Lemma 3.5.9 Λ is a finite set. Therefore the set of zero-divisors of $\bar{R}$ is $P_1 \cup \cdots \cup P_m$. In other words the set of regular elements of

$\bar{R}$ is $\bar{R}\setminus(P_1\cup\cdots\cup P_m)$. Suppose $\bar{z}_{i+1}\in P_1$, then by Theorem 3.7.16 $\dim(\bar{R}/\bar{R}\bar{z}_{i+1}) = \dim\bar{R}$. Therefore $\dim(R/\sum_{j=1}^{i+1} Rz_j) = \dim(R/\sum_{j=1}^{i} Rz_j)$. By using Lemma 3.5.17 we get $\dim(R/\sum_{j=1}^{r} Rz_j) > n-r$ which is a contradiction. Therefore $\bar{z}_{i+1}$ is not in any minimal prime ideal and so z_{i+1} is regular modulo $\sum_{j=1}^{i} Rz_j$. □

Notice that a similar result holds when instead of a finitely generated graded algebra we consider a Noetherian local ring. See Theorem 21.2 and the definition of complete intersection for a Noetherian local ring on page 171 of [30].

Corollary 3.8.3. *A graded complete intersection finitely generated graded algebra is Gorenstein and hence Cohen-Macaulay.*

Proof. Let $R = F[X_1,\ldots,X_n]$ and $S = R/J$ where J has minimal generating set $\{z_1,\ldots,z_r\}$ and $\dim S = n-r$. We claim that S is Gorenstein. Since R is Gorenstein by Corollary 3.7.22 and by the above theorem, $\{z_1,\ldots,z_r\}$ is a regular sequence. Thus by Theorem 3.7.25, S is Gorenstein. □

We are now going to state a useful result.

Lemma 3.8.4. *(Corollary 5.4.4 in [39]). Suppose that G is a finite group, F a field and V a finite-dimensional FG-module. Then the Krull dimension of $F[V]^G$ is equal to $\dim_F V$.*

Remark 3.8.5. By the above lemma, Theorem 2.2.4, Theorem 2.4.13, Theorem 2.4.14, Theorem 2.3.17 and Theorem 2.3.18, the invariant rings of symplectic, orthogonal (in the odd characteristic case) and unitary groups are graded complete intersections, and so in particular these are Gorenstein and Cohen-Macaulay.

Remark 3.8.6. It should be noted that in section 8 of [40] Stanley defines Gorenstein rings. He discusses the work of other authors. Some of these authors describe necessary conditions and some of them describe both necessary and sufficient conditions for Gorenstein rings. Then he summarizes this work in Theorem 8.1 which gives equivalent conditions for Gorenstein rings. In particular Stanley's account can be used to show that graded complete intersections are Gorenstein.

Chapter 4

Invariant rings of $\mathbf{Aut}(V, \xi)$, $\mathbf{Aut}(V, H)$ and $\mathbf{Aut}(V, Q)$

Let V be a vector space over the finite field F_q. Suppose $S = F_q[V]$ is the symmetric algebra on V^*. In chapter 2 we discussed the ring of invariants S^G in the cases when G is the the symplectic, unitary or orthogonal group (the latter in the odd characteristic case). In this chapter we shall find the ring of invariants of the following groups.

$$\mathrm{Aut}(V, \xi) = \{g \in GL(V) : \xi(gv_1, gv_2) = \xi(v_1, v_2) \ \forall \ v_1, v_2 \in V\}$$

$$\mathrm{Aut}(V, H) = \{g \in GL(V) : H(gv_1, gv_2) = H(v_1, v_2) \ \forall \ v_1, v_2 \in V\}$$

$$\mathrm{Aut}(V, Q) = \{g \in GL(V) : Q(gv) = Q(v) \ \forall \ v \in V\}$$

where ξ is a singular alternating form, H is a singular hermitian form and Q is a singular quadratic form.

4.1 Group actions

We defined group action in chapter 1. Here we describe some results related to group actions which we shall use in our main results.

Lemma 4.1.1. *If G acts on X and $N \lhd G$ then G/N acts on X^N and $(X^N)^{G/N} = X^G$.*

Proof. For $x \in X^N$, define $gN \cdot x = g \cdot x$. This is well defined because if $g_1N = g_2N$, then $g_1^{-1}g_2 \in N$. Therefore $g_1^{-1}g_2 \cdot x = x$ and so $g_1 \cdot x = g_2 \cdot x$. So we have an action of G/N on X^N. The second statement is clear. □

Lemma 4.1.2. *Let G_1, G_2 be two groups and S_1, S_2 be two rings. Suppose G_1 acts on S_1 and G_2 acts on S_2. Then $G_1 \times G_2$ acts on $S_1 \otimes S_2$.*

Proof. Define a map $S_1 \otimes S_2 \times (G_1 \times G_2) \to S_1 \otimes S_2$ by $(s_1 \otimes s_2)^{(g_1,g_2)} = s_1^{g_1} \otimes s_2^{g_2}$ where $s_1 \otimes s_2 \in S_1 \otimes S_2$ and $(g_1, g_2) \in G_1 \times G_2$. We can easily show that this is an action. □

4.2 Integrally closed domains

In this section we define integrally closed domains. We defined unique factorization domain in chapter 2. Here we show that every unique factorization domain is integrally closed. At the end of this section we shall show that every polynomial ring in two or more indeterminates (up to a finite number of indeterminates) can be written as a tensor product of two polynomial rings.

Definition 4.2.1. An integral domain R is said to be *integrally closed* if every element θ of its field of fractions $ff(R)$ which satisfies a monic polynomial with coefficients in R is already in R itself.

Lemma 4.2.2. *If $R \subseteq R_1 \subseteq S$ are integral domains such that*

(i) S is integral over R

(ii) $ff(R) = ff(R_1)$

(iii) R is integrally closed

then $R = R_1$.

Proof. Let $\alpha \in R_1$. By (i) choose a monic polynomial $f(X)$ in $R[X]$ such that $f(\alpha) = 0$. By (ii) $\alpha \in ff(R)$ and so by (iii) $\alpha \in R$. □

Lemma 4.2.3. *If R is a UFD, then R is integrally closed.*

Proof. Let R be a UFD with $ff(R)$ the field of fractions. Let $u \in ff(R)$ be integral over R. Then for some $a_0, \ldots, a_{n-1} \in R$,

$$u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$$

where $u = \dfrac{c}{d}$ for some $c, d \in R$ and c, d have no non-unit common divisor. Multiplying both sides of the above equation by d^n, we get

$$c^n + a_{n-1}dc^{n-1} + \cdots + a_0 d^n = 0.$$

Thus

$$c^n = -d(a_{n-1}c^{n-1} + \cdots + a_0 d^{n-1}).$$

Now since R is a UFD, d must divide c. But c and d have no non-unit common divisor so $d = \pm 1$. Therefore $u \in R$ and so R is integrally closed. □

Lemma 4.2.4. *Let F be a field. Then*

$$F[X_1, \ldots, X_n, X_{n+1}, \ldots, X_{n+m}] \cong F[X_1, \ldots, X_n] \otimes F[X_{n+1}, \ldots, X_{n+m}].$$

Proof. R.H.S $= F[X_1 \otimes 1, \ldots, X_n \otimes 1, 1 \otimes X_{n+1}, \ldots, 1 \otimes X_{n+m}]$. Define a map by $X_1 \mapsto X_1 \otimes 1, \ldots, X_n \mapsto X_n \otimes 1$ and $X_{n+1} \mapsto 1 \otimes X_{n+1}, \ldots, X_{n+m} \mapsto 1 \otimes X_{n+m}$. Then we can check that this is an isomorphism. □

4.3 The Fundamental Theorem of Galois Theory

A good introduction to Galois Theory is given in [41]. We give a brief summary here.

Definition 4.3.1. If F is a field and f is a polynomial over F, then f *splits* over F if it can be expressed as a product of linear factors $f(t) = c(t - \alpha_1)\ldots(t - \alpha_n)$ where $c, \alpha_1, \ldots, \alpha_n \in F$.

Definition 4.3.2. Let F be a field and let Σ be an extension of F. Then Σ is a *splitting field* for the polynomial f over F if

(i) f splits over Σ and

(ii) If $F \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

The second condition is clearly equivalent to:

(iii) $\Sigma = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the zeros of f in Σ.

Definition 4.3.3. A field extension E/F is *normal* if every irreducible polynomial f over F that has at least one zero in E splits in E.

Theorem 4.3.4. *(Theorem 17.10 in [41]). A field extension E/F is normal and finite if and only if E is a splitting field for some polynomial over F.*

Definition 4.3.5. An irreducible polynomial f over a field F is *separable* over F if it has no multiple zero in a splitting field.

Definition 4.3.6. (i) An arbitrary polynomial over a field F is separable over F if all its irreducible factors are separable over F. Otherwise, it is an inseparable polynomial.

(ii) If E/F is an extension, then an algebraic element $\alpha \in E$ is separable over F if its minimal polynomial over F is separable over F. Otherwise, α is an inseparable elements.

(iii) An algebraic extension E/F is a separable extension if every $\alpha \in E$ is separable over F. Otherwise, it is an inseparable extension.

Theorem 4.3.7. *(Theorem 17.22 in [41]). If E/F is a field extension such that E is generated over F by a set of separable algebraic elements, then E/F is separable.*

Definition 4.3.8. Let E/F be a field extension. A *F-automorphism* of E is an automorphism δ of E such that $\delta(c) = c$ for all $c \in F$. We say δ fixes $c \in F$.

Theorem 4.3.9. *(Theorem 8.2 in [41]). If E/F is a field extension, then the set of all F-automorphisms of E forms a group under composition of maps.*

Definition 4.3.10. The *Galois group* $\mathrm{Gal}(E/F)$ of a field extension E/F is the group of all F-automorphisms of E under the operation of composition of maps.

The importance of the Galois group is made clear by the fact that, under certain extra hypotheses, we get a one-to-one correspondence between:

(i) Subgroups of $\mathrm{Gal}(E/F)$ and

(ii) Subfields M of E such that $F \subseteq M$.

If E/F is a field extension, we call any field M such that $F \subseteq M \subseteq E$ an intermediate field. To each intermediate field we associate the group $\mathrm{Gal}(E/M)$ of all M-automorphisms of E. Thus $\mathrm{Gal}(E/F)$ is the whole Galois group, and $\mathrm{Gal}(E/E) = 1$, the group consisting of just the identity map of E. Clearly, if $M \subseteq N$, then $\mathrm{Gal}(E/M) \supseteq \mathrm{Gal}(E/N)$ because any automorphism of E which fixes the elements of N certainly fixes the elements of M.

Conversely, to each subgroup H of $\mathrm{Gal}(E/F)$ we associate the set

$$\mathrm{Fix}(H) = \{x \in E : \delta(x) = x \ \forall \ \delta \in H\}.$$

This is the fixed field of H.

Lemma 4.3.11. *(Lemma 8.5 in [41]). If H is a subgroup of* $\mathrm{Gal}(E/F)$*, then* $\mathrm{Fix}(H)$ *is a subfield of E containing F.*

It is easy to see that if $H \subseteq H'$, then $\mathrm{Fix}(H) \supseteq \mathrm{Fix}(H')$. Let E/F be a field extension with Galois group G. Let $\mathcal{F}$ be the set of intermediate fields and let $\mathcal{G}$ be the set of all subgroups H of G.

Theorem 4.3.12. *(Fundamental Theorem of Galois Theory: Theorem 17.23 in [41]). Let E/F be a finite separable normal field extension, with Galois group G. Let $H \in \mathcal{G}$ and $M \in \mathcal{F}$ where $\mathcal{G}$ and $\mathcal{F}$ are as defined above. Then*

(i) The Galois group G has order $[E : F]$.

(ii) The maps

$$M \mapsto \mathrm{Gal}(E/M),$$

$$H \mapsto \mathrm{Fix}(H),$$

are mutual inverses, and set up an order-reversing one-to-one correspondence between $\mathcal{F}$ and $\mathcal{G}$.

(iii) $[E : M] = |\mathrm{Gal}(E/M)|$ *and* $[M : F][E : M] = |G|$.

(iv) M/F is a normal extension if and only if $\mathrm{Gal}(E/M)$ *is a normal subgroup of G.*

(v) If M/F is a normal extension, then the Galois group of M/F is isomorphic to the quotient group $G/\mathrm{Gal}(E/M)$.

We now give an important result which will be used in later sections.

Proposition 4.3.13. *(Proposition 1.2.4 in [39]). Suppose V is a finite dimensional faithful representation of a finite group G over a field F. Let $S = F[V]$, then $ff(S)$ is a Galois (i.e., normal and separable) extension of $ff(S)^G$ with Galois group G. The field $ff(S)^G$ is the field of fractions of S^G, and S^G is integrally closed in $ff(S)^G$.*

4.4 Algebraically independent elements

In this section we define algebraically independent elements and transcendental degrees. We state some properties of these. The results in this section have been taken from [4], [30], [39] and [43]. We shall use these results in this chapter as well as in chapter 5.

Definition 4.4.1. A set of polynomials is called *algebraically independent* if there are no algebraic relations between them.

The following result gives us a sufficient condition for algebraically independent elements. Note that in Proposition 5.21 of [33] the author proves this result over the complex field.

Lemma 4.4.2. *(Lemma 5.6.1 in [39]). Let F be a field. If $f_1, \ldots, f_n \in F[z_1, \ldots, z_n]$ and*

$$\begin{vmatrix} \frac{\partial f_1}{\partial z_1} & \cdots & \frac{\partial f_n}{\partial z_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial z_n} & \cdots & \frac{\partial f_n}{\partial z_n} \end{vmatrix} \neq 0$$

then $f_1, \ldots, f_n$ are algebraically independent.

Definition 4.4.3. Let E/F be a field extension. The largest cardinality of an algebraically independent subset of E over F is called the *transcendental degree* of E over F. It is denoted by $\mathrm{tr.deg}_F E$.

Lemma 4.4.4. *(Theorem 5.6 in [30]). Let F be a field and R an integral domain which is finitely generated over F, then*

$$\dim R = \mathrm{tr.\,deg}_F(ff(R)).$$

Note that if $R_1 \subseteq R_2$ are integral domains which are finitely generated over F, then it follows from the above lemma that $\dim R_1 \leq \dim R_2$.

Proposition 4.4.5. *(Proposition 5.4.2 in [4]) Let $x_1, \ldots, x_n$ be algebraically independent indeterminates over a perfect field F. If $f_1, \ldots, f_n$ are elements of $F(x_1, \ldots, x_n)$, then $F(f_1, \ldots, f_n) \subseteq F(x_1, \ldots, x_n)$ is a finite separable extension if and only if*

$$\begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix} \neq 0.$$

It follows from the above proposition and Lemma 4.4.2 that if $F(f_1, \ldots, f_n) \subseteq F(x_1, \ldots, x_n)$ is a finite separable extension then $f_1, \ldots, f_n$ are algebraically independent.

Lemma 4.4.6. *(Lemma 3.2 in [43]) Let V be a vector space over the field F_q. Suppose $S = F_q[x_1, \ldots, x_n]$ is the symmetric algebra on V^*. Let $R = F_q[z_1, \ldots, z_n]$ where z_i are a set of algebraically independent polynomials in x_i. Then the degree of the field extension $ff(R) \subseteq ff(S)$ is $\prod \deg z_i$.*

4.5 Laurent expansion and Poincaré series

In this section we define Laurent expansions and Poincaré series. We state some properties of these. We shall not use the results in this section in the thesis but they are very important in invariant theory.

Definition 4.5.1. A *Laurent expansion* about $t = 1$ with coefficients in a field F is an expression of the form

$$P = \sum_k p_k(1-t)^k$$

where $p_k \in F$ and $k \in \mathbb{Z}$.

Definition 4.5.2. Let F be a field. Suppose that $R = \bigoplus_{j=0}^{\infty} R_j$ is a commutative graded ring with $R_0 = F$, and finitely generated over F by homogeneous elements $x_1, \ldots x_s$ in positive degree $k_1, \ldots, k_s$. Suppose that $M = \bigoplus_{j=-\infty}^{\infty} M_j$ is a finitely generated graded R-module. The Poincaré series of M is defined as follows

$$P(M,t) = \sum_{j\in\mathbb{Z}} \dim_F(M_j)t^j.$$

We now give some examples.

Example 4.5.3.

(i) $P(F_q[X],t) = 1 + t + t^2 + \ldots$ *and* $1 + t + t^2 + \cdots = \dfrac{1}{1-t}$.

(ii) $P(F_q[X_1, \ldots, X_n], t) = \dfrac{1}{(1-t)^n}$.

(iii) $P(F_q[Y_1, \ldots, Y_n], t) = \prod_{i=1}^{n} \dfrac{1}{(1-t^{d_i})}$ *where* $d_i = \deg Y_i$ *for* $i = 1, \ldots, n$.

Before giving the notion of degree for a finitely generated commutative graded F-algebra $R = \bigoplus_{j=0}^{\infty} R_j$ with $R_0 = F$ we are going to state some useful properties of Poincaré series. The following two results have been taken from [4].

Theorem 4.5.4. *(Theorem 2.1.1 in [4]). Let R and M be as in Definition 4.5.2. Then the Poincaré series $P(M,t)$ is of the form*

$$\frac{f(t)}{\prod_{j=1}^{s}(1-t^{k_j})}$$

where $f(t)$ is a polynomial in t with integer cofficients.

Theorem 4.5.5. *(Theorem 2.2.7 in [4]). Let R and M be as in Definition 4.5.2. Then there exists homogeneous element $f_1,\ldots,f_n$ of positive degree in R, which generate a polynomial subring $F[f_1,\ldots,f_n]$ in $R/ann(M)$ over which M is finitely generated as a module. The number n is equal to the order of the pole at $t=1$ of $P(M,t)$ and is also equal to the krull dimension of M.*

Definition 4.5.6. Let $R=\bigoplus_{j=0}^{\infty}R_j$ be a finitely generated commutative graded F-algebra with $R_0=F$. If the Krull dimension is n, then the value of the rational function $(1-t)^nP(R,t)$ at $t=1$ is a non-zero rational number, called the *degree* of R, written as $\deg(R)$. More generally, if $M=\bigoplus_{-\infty}^{\infty}M_j$ is a finitely generated graded R-module, we define the rational number $\deg(M)$ by the Laurent expansion about $t=1$:

$$P(M,t)=\frac{\deg(M)}{(1-t)^n}+\ldots.$$

To explain the above concept we give some examples.

Example 4.5.7.

(i) $\deg(F_q[X_1,\ldots,X_n])=1$.

(ii) $\deg(F_q[Y_1,\ldots,Y_n])=\dfrac{1}{\prod_{i=1}^{n}d_i}$ *where* $d_i=\deg Y_i$ *for* $i=1,\ldots,n$.

We know that $P(F_q[Y_1,\ldots,Y_n],t)=\displaystyle\prod_{i=1}^{n}\frac{1}{(1-t^{d_i})}$. Let us expand this in a Laurent expansion about $t=1$. First note that

$$\prod_{i=1}^{n}\frac{1}{(1-t^{d_i})}=\frac{1}{(1-t)^n}\prod_{i=1}^{n}\frac{1}{(1+t+\cdots+t^{d_i-1})}$$

and $\prod_{i=1}^{n}\dfrac{1}{(1+t+\cdots+t^{d_i-1})}=\dfrac{1}{\prod_{i=1}^{n}d_i}$ when $t=1$. Therefore

$$P(F_q[Y_1,\ldots,Y_n],t)=\frac{1}{\prod_{i=1}^{n}d_i}\cdot\frac{1}{(1-t)^n}+\ldots$$

Let us describe some properties.

Lemma 4.5.8. *(Theorem 5.5.3 in [39]). Suppose that G is a finite group and V is an n-dimensional faithful representation of G over a field F. Then* $\deg(F[V]^G)=\frac{1}{|G|}$. *Hence the Laurent expansion of the Poincaré series of $F[V]^G$ about $t=1$ is*

$$P(F[V]^G,t)=\frac{1}{|G|(1-t)^n}+\ldots$$

Lemma 4.5.9. *Let $H = F[f_1,\ldots,f_m]/\langle h_1,\ldots,h_k\rangle$, where $h_1,\ldots,h_k$ is a regular sequence of homogeneous elements in $F[f_1,\ldots,f_m]$. If $\deg f_j = l_j$ and $\deg h_i = n_i$, then*

$$P(H,t) = \frac{\prod_{i=1}^{k}(1-t^{n_i})}{\prod_{j=1}^{m}(1-t^{l_j})}.$$

Proof. Clear. □

Thus by expanding this in a Laurent expansion about $t = 1$, we get

$$P(H,t) = \frac{\prod_{i=1}^{k} n_i}{\prod_{j=1}^{m} l_j}\frac{1}{(1-t)^{m-k}} + \ldots.$$

Note that in Proposition 3.3.2 in [34] the authors take $h_1,\ldots,h_k$ to be algebraically independent and $F[f_1,\ldots,f_m]$ to be a free $F[h_1,\ldots,h_k]$-module and get the same result.

4.6 The invariant ring S^N

Let V be a vector space over the field F_q. In this section we want to compute the invariant ring S^N where $S = F_q[V]$ and we shall define N in the following discussion. Consider

$$0 \leq U \leq V$$

Let $e_1,\ldots,e_m$ be a basis of U, extend this to the basis $e_1,\ldots,e_m,e_{m+1},\ldots,e_{m+n}$ of V. Let

$$G = \{g \in GL(V) : gU = U\}.$$

Suppose $x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+n}$ is the corresponding dual basis of V^*. Now define

$$\phi : G \to GL(U) \times GL(V/U)$$

by

$$g \mapsto (g|_U,\ \bar{g})$$

where $\bar{g}(v+U) = gv+U$. Then ϕ is a homomorphism. Let $N = \mathrm{Ker}\phi$ where

$$\mathrm{Ker}\phi = \{g \in G : gu = u\ \forall\ u \in U \text{ and } gv - v \in U\ \forall\ v \in\ V\}.$$

The matrix of N is

$$\begin{bmatrix} I_U & * \\ 0 & I_{V/U} \end{bmatrix}.$$

Now if $g \in N$, then $x_{m+i}^g = x_{m+i}$ for $1 \leq i \leq n$. Fix i with $1 \leq i \leq m$, then $x_i^g = x_i +$ something in $(V/U)^*$. Now

$$\underset{(V/U)}{D}(x_i) = \prod_{x \in (V/U)^*} (x_i - x) \in S^N \text{ when } 1 \leq i \leq m.$$

Suppose

$$R = F_q[y_1, \ldots, y_m, x_{m+1}, \ldots, x_{m+n}] \text{ where } y_i = \underset{(V/U)}{D}(x_i) \text{ for } 1 \leq i \leq m.$$

Now $R \subseteq S^N \subseteq S$.

(i) We need to show that S is integral over R. This is true because for $x_i \in S$, where $m+1 \leq i \leq m+n$, there exist polynomials $P_i(X) = X - x_i \in R[X]$ such that $P_i(x_i) = 0$. Now for $x_j \in S$, where $1 \leq j \leq m$, there exist polynomials $P_j(X) = \underset{(V/U)}{D}(X - x_j) \in R[X]$ such that $P_j(x_j) = 0$.

(ii) We need to show that $ff(R) = ff(S^N)$. Obviously $ff(R) \subseteq ff(S^N)$. Thus we need to show that $ff(S^N) \subseteq ff(R)$. For this we need to check $ff(R) \subseteq ff(S)$ is finite separable normal field extension. The polynomials

$$P_j(X) = \underset{(V/U)}{D}(X - x_j) \text{ for } 1 \leq j \leq m$$

split over $ff(S)$, where these $P_j(X) \in R[X]$, and it is easy to see that

$$ff(S) = ff(R)(x_1, \ldots, x_m).$$

Thus by definition $ff(S)$ is a splitting field for these polynomials and so by Theorem 4.3.4 the extension $ff(R) \subseteq ff(S)$ is finite and normal. Now the elements $x_1, \ldots, x_m$ are separable. Therefore by Theorem 4.3.7 the extension $ff(R) \subseteq ff(S)$ is separable. Let H be the Galois group of the field extension $ff(R) \subseteq ff(S)$. On the other hand Proposition 4.3.13 shows that the field extension $ff(S^N) \subseteq ff(S)$ is Galois with Galois group N. Thus by Theorem

4.3.12 $N \subseteq H$. Since the extension $ff(R) \subseteq ff(S)$ is finite and separable, so by the remark after Proposition 4.4.5 we have that $y_1, \ldots, y_m, x_{m+1} \ldots, x_{m+n}$ are algebraically independent. Therefore by Lemma 4.4.6 and Theorem 4.3.12 part (ii) $\mid H \mid = \prod \deg y_i$ but $\mid N \mid = \prod \deg y_i$. Thus $H = N$ and so by Theorem 4.3.12 $ff(R) = ff(S^N)$.

(iii) From the discussion in (ii) it is clear that $R = F_q[y_1, \ldots, y_m, x_{m+1}, \ldots, x_{m+n}]$ is a polynomial ring. Thus by Lemma 2.3.16 and Lemma 4.2.3 R is integrally closed. Therefore according to Lemma 4.2.2 we have

$$S^N = F_q[y_1, \ldots, y_m, x_{m+1}, \ldots, x_{m+n}].$$

Now consider the chain of subspaces of V below.

$$0 = U_0 \leq U_1 \leq \cdots \leq U_n = V.$$

Let $m_i = \dim_{F_q} U_i/U_{i-1}$ for each i so that $\dim_{F_q} V = m_1 + \cdots + m_n$. Let $e_1, \ldots, e_{m_1+\cdots+m_n}$ be a basis of V chosen by successively extending bases of the U_i so that $e_1, \ldots, e_{m_1+\cdots+m_i}$ is a basis of U_i. Let $x_1, \ldots, x_{m_1+\cdots+m_n}$ denote the dual basis of V^*. The chain of subspaces of V gives rise to a natural chain of subspaces in V^*:

$$0 = (V/U_n)^* \leq (V/U_{n-1})^* \leq \cdots \leq (V/U_0)^* = V^*$$

in which $(V/U_i)^*$ has dimension $m_{i+1}+\cdots+m_n$ and basis $x_{m_1+\cdots+m_i+1}, \ldots, x_{m_1+\cdots+m_n}$. For definiteness we shall assume that $m_i \geq 1$ for each i so that the inclusions in our chains of subspaces are strict.

Associated to any subspace W of V there is the Dickson polynomial $D_{(V/W)}(X)$ in $F[V][X]$ as defined in Definition 2.1.1 and which has degree equal to the order of $(V/W)^*$. Thus we have $\deg D_{(V/U_i)}(X) = |(V/U_i)^*| = q^{m_{i+1}+\cdots+m_n}$. We are interested in the rings of invariants of two groups. First, the group

$$G := \{g \in GL(V) : \ gU_i = U_i \ \forall \ i\}$$

and secondly the kernel N of the natural surjective map

$$G \to GL(U_1) \times GL(U_2/U_1) \times \cdots \times GL(U_n/U_{n-1})$$

Note that the order of N is q^d where

$$d = \sum_{1 \le i < j \le n} m_i m_j.$$

We shall use Propositions 4.5.5 and 4.5.6 of [34] to compute the ring of invariants of N. It will obviously work when $n = 2$ which we have done above by a different method. We have used a different method in our above discussion for $n = 2$ because we shall use part (ii) of the above discussion in chapter 5. Firstly we are going to define homogeneous system of parameters. The following definition have been taken from [40].

Definition 4.6.1. Let F be a field. Suppose $R = \bigoplus_{j=0}^{\infty} R_j$ is a finitely generated commutative graded F-algebra with $R_0 = F$. If the Krull dimension is n, then a set $f_1, \ldots, f_n$ of homogenous elements of positive degree is said to be *homogeneous system of parameters* if R is finitely generated module over the subalgebra $F[f_1, \ldots, f_n]$

Lemma 4.6.2. *The polynomials* $y(i,\ell) := D_{(U_{i+1}/U_i)} \ldots (D_{(V/U_{n-1})}(x_\ell))$ *and* $x_{m_1+\cdots+m_{n-1}+j}$ *generate the ring of invariants* S^N*, where* $1 \le i \le n-1$, $1 \le j \le m_n$ *and* $m_1 + \cdots + m_{i-1} < \ell \le m_1 + \cdots + m_i$*. [Note that* $m_1 + \cdots + m_{i-1}$ *should be interpreted as* 0 *when* $i = 1$*.]*

Proof. We need to show that the $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$ form a homogeneous system of parameters. The number of $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$ is $\sum_i m_i = \dim V$ and the product of their degrees is q^d where

$$d = m_1(m_2 + \cdots + m_n) + m_2(m_3 + \cdots + m_n) + \cdots + m_{n-1}m_n = \sum_{1 \le i < j \le n} m_i m_j.$$

The result then follows from Proposition 4.5.5 of [34] .

In order to prove that $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$ form a homogeneous system of parameters, the key step, just as in Neusel and Smith's proof of the Nakajima–Stong Theorem (Proposition 4.5.6 of [34]) is to show that $F_q[V]$ is integral over the ring generated by the $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$. First we show that $y(i,\ell)$ and

$x_{m_1+\cdots+m_{n-1}+i}$ are invariants and $F_q[V]$ is integral over the ring generated by the $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$.

If $g \in N$, then clearly $x^g_{m_1+\cdots+m_{n-1}+i} = x_{m_1+\cdots+m_{n-1}+i}$ for $1 \leq i \leq m_n$. The $y(n-1,\ell) := D_{(V/U_{n-1})}(x_\ell)$ where ℓ in the range $m_1+\cdots+m_{n-2} < \ell \leq m_1+\cdots+m_{n-1}$ all belong to the ring of invariants S^N. To see this, suppose that g is any element of N. Then for any $x \in (V/U_{n-2})^*$ we have $x^g = x + z$ for some $z = z(x,g)$ belonging to $(V/U_{n-1})^*$. The additive behaviour of the Dickson polynomials yields

$$D_{(V/U_{n-1})}(x^g) = D_{(V/U_{n-1})}(x+z) = D_{(V/U_{n-1})}(x) + D_{(V/U_{n-1})}(z)$$

and since $D_{(V/U_{n-1})}$ vanishes on $(V/U_{n-1})^*$ we have $D_{(V/U_{n-1})}(z) = 0$. Therefore

$$D_{(V/U_{n-1})}(x)^g = D_{(V/U_{n-1})}(x^g) = D_{(V/U_{n-1})}(x).$$

This shows that the $y(n-1,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-2} < \ell \leq m_1+\cdots+m_{n-1}$ are invariant as claimed. Let R_1 be the ring generated by the $y(n-1,\ell)$ where ℓ in the range $1 \leq \ell \leq m_1+\cdots+m_{n-1}$, and $x_{m_1+\cdots+m_{n-1}+j}$ where $1 \leq j \leq m_n$. Then $F_q[V]$ is integral over R_1. In order to prove that it suffices to check that each x_i satisfies a monic polynomial with coefficients in the ring R_1. For $x_j \in F_q[V]$, where $m_1+\cdots+m_{n-1}+1 \leq j \leq m_1+\cdots+m_n$, there exist polynomials $P_j(X) = X - x_j \in R_1[X]$ such that $P_j(x_j) = 0$. Now for $x_j \in F_q[V]$, where $1 \leq j \leq m_1+\cdots+m_{n-1}$, there exist polynomials $P_j(X) = D_{(V/U_{n-1})}(X - x_j) \in R_1[X]$ such that $P_j(x_j) = 0$. Now for each of dual space U_i^* there is a natural short exact sequence

$$0 \to (U_i/U_{i-1})^* \to U_i^* \to U_{i-1}^* \to 0.$$

We are going to identify each of the spaces U_i^* with a certain subspace of the symmetric algebra $F_q[V]$. First, U_n^* is identified with V^*, the degree one component of the symmetric algebra. Now the Dickson polynomial

$$D_{(V/U_{n-1})}(X) = \prod_{x \in (V/U_{n-1})^*} (X - x)$$

determines a linear function $V^* \to F[V]$ with kernel $(V/U_{n-1})^*$. Hence it is natural to identify U_{n-1}^* with $D_{(V/U_{n-1})}(V^*)$. This has the effect that elements of U_{n-1}^* have

natural degree equal to the degree of $D_{(V/U_{n-1})}$. [Note that the degree of $D_{(V/U_{n-1})}$ is equal to the order of the vector space $(V/U_{n-1})^*$]. We may then define like this:

$$D_{(U_{n-1}/U_{n-2})}(X) = \prod_{x \in (U_{n-1}/U_{n-2})^*} (X - x).$$

Then $D_{(U_{n-1}/U_{n-2})}$ is a homogeneous polynomial provided we agree that the free variable X has degree equal to the degree of $D_{(V/U_{n-1})}$. Just as $D_{(V/U_{n-1})}$, the new polynomial $D_{(U_{n-1}/U_{n-2})}$ defines a linear map from U_{n-1}^* to the symmetric algebra with kernel $(U_{n-1}/U_{n-2})^*$ and its image may be identified with U_{n-2}^*. The degree of $D_{(U_{n-1}/U_{n-2})}$ is equal to the order of the vector space $(V/U_{n-2})^*$. Continuing in this way we define Dickson polynomials $D_{(U_{n-i+1}/U_{n-i})}$ for each i, each one determining a linear map with domain U_{n-i+1}^*, kernel $(U_{n-i+1}/U_{n-i})^*$ and image identified with U_{n-i}^*. The degree of $D_{(U_{n-i+1}/U_{n-i})}$ is equal to the order of the vector space V/U_{n-i}.

Now U_{n-1}^* is identified with the subspace generated by the $y(n-1,\ell)$ where ℓ in the range $1 \leq \ell \leq m_1 + \cdots + m_{n-1}$. By the same argument above the elements $D_{(U_{n-1}/U_{n-2})}(y(n-1,\ell))$ where ℓ in the range $m_1+\cdots+m_{n-3} < \ell \leq m_1+\cdots+m_{n-2}$ are invariants of N. This means that the $y(n-2,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-3} < \ell \leq m_1+\cdots+m_{n-2}$ are invariants of N. Let R_2 be the ring generated by $x_{m_1+\cdots+m_{n-1}+i}$ where $1 \leq j \leq m_n$, $y(n-1,\ell)$ where $m_1+\cdots+m_{n-2} < \ell \leq m_1+\cdots+m_{n-1}$ and $y(n-2,\ell)$ where ℓ in the range $1 \leq \ell \leq m_1+\cdots+m_{n-2}$. Then R_1 is an integral over R_2. For $x_j \in R_1$, where $m_1+\cdots+m_{n-1}+1 \leq j \leq m_1+\cdots+m_n$, there exist polynomials $P_j(X) = X - x_j \in R_2[X]$ such that $P_j(x_j) = 0$. Now for $y(n-1,\ell) \in R_1$ where $m_1+\cdots+m_{n-2} < \ell \leq m_1+\cdots+m_{n-1}$, there exist polynomials $P_\ell(X) = X - y(n-1,\ell) \in R_1[X]$ such that $P_\ell(y(n-1,\ell)) = 0$. For $y(n-1,\ell) \in R_1$, where $1 \leq \ell \leq m_1+\cdots+m_{n-2}$, there exist polynomials $P_\ell(X) = D_{(U_{n-1}/U_{n-2})}(X - y(n-1,\ell)) \in R_2[X]$ such that $P_\ell(y(n-1,\ell)) = 0$.

Now U_{n-2}^* is identified with the subspace generated by the elements $y(n-2,\ell))$ where ℓ in the range $1 \leq \ell \leq m_1+\cdots+m_{n-2}$. Now by the same argument above $D_{(U_{n-2}/U_{n-3})}((y(n-2,\ell))$ where ℓ in the range $m_1+\cdots+m_{n-4} < \ell \leq m_1+\cdots+m_{n-4}+m_{n-3}$ are invariants of N. This means that $y(n-3,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-4} < \ell \leq m_1+\cdots+m_{n-4}+m_{n-3}$ are invariants. Let R_3 be the ring

generated by the $x_{m_1+\cdots+m_{n-1}+i}$ where $1 \leq j \leq m_n$, $y(n-2,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-3} < \ell \leq m_1+\cdots+m_{n-2}$ and $y(n-3,\ell)))$ where ℓ in the range $1 \leq \ell \leq m_1+\cdots+m_{n-3}$. Then by the same method as above R_2 is integral over R_3. By induction we would get a ring which we let R_{n-2} and R_{n-2} is generated by $x_{m_1+\cdots+m_{n-1}+i}$ where $1 \leq j \leq m_n$, $y(n-1,\ell)$ where $m_1+\cdots+m_{n-2} < \ell \leq m_1+\cdots+m_{n-1}$, $y(n-2,\ell))$ where ℓ in the range $m_1+\cdots+m_{n-3} < \ell \leq m_1+\cdots+m_{n-2}$, $y(n-3,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-4} < \ell \leq m_1+\ldots m_{n-3}$, $\ldots$, $y(2,\ell)$ where ℓ in the range $1 \leq \ell \leq m_1+m_2$.

Now U_2^* is identified with the subspace generated by the $y(2,\ell)$ where $1 \leq \ell \leq m_1+m_2$. By the same argument above $D_{(U_2/U_1)}(y(2,\ell))$ where ℓ in the range $0 < \ell \leq m_1$ are invariants of N. This means that $y(1,\ell)$ where ℓ in the range $0 < \ell \leq m_1$ are invariants. Let R_{n-1} is generated by $x_{m_1+\cdots+m_{n-1}+i}$ where $1 \leq j \leq m_n$, $y(n-1,\ell)$ where $m_1+\cdots+m_{n-2} < \ell \leq m_1+\cdots+m_{n-1}$, $y(n-2,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-3} < \ell \leq m_1+\cdots+m_{n-2}$, $y(n-3,\ell)$ where ℓ in the range $m_1+\cdots+m_{n-4} < \ell \leq m_1+\ldots m_{n-3}$,$\ldots$,$y(2,\ell)$ where ℓ in the range $m_1 \leq \ell \leq m_2$, $y(1,\ell)$ where ℓ in the range $0 < \ell \leq m_1$. Again by the same way R_{n-2} is integral over R_{n-1}. It follows that $F[V]$ is integral over R_{n-1}.

Next, consider the number of $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$ and their degrees. For each i there are m_i possible values of ℓ and so the number of generators $y(i,\ell)$ and $x_{m_1+\cdots+m_{n-1}+i}$ is $\sum_i m_i = \dim V$. The degree of $y(i,\ell)$ is equal to the product of the degrees of $D_{(U_{i+1}/U_i)},\ldots,D_{(V/U_{n-1})}$ which is $q^{m_{i+1}+\cdots+m_n}$. The degree of $x_{m_1+\cdots+m_{n-1}+i}$ is one. Thus product of the degrees of all generators is q^d where

$$d = m_1(m_2+\cdots+m_n)+m_2(m_3+\cdots+m_n)+\cdots+m_{n-1}m_n = \sum_{1\leq i<j\leq n} m_i m_j.$$

□

Lemma 4.6.3. *Let* $G_1 = \{g \in GL(V) : gU = U\}$ *where* $U = \mathrm{Rad}\xi$ *and* $G_2 = \mathrm{Aut}(V,\xi)$. *Then the maps* $\phi_1 : G_1 \to GL(U)\times GL(V/U)$ *and* $\phi_2 : G_2 \to GL(U)\times GL(V/U)$ *have the same kernels.*

Proof. First we need to show that $G_2 \leq G_1$. For this let $g \in G_2$, then $\xi(gw,gv) = \xi(w,v)$ for all $w,v \in V$. Now let $u \in U$, then $\xi(gu,v) = \xi(u,g^{-1}v) = 0$ for all $v \in V$.

Thus $gu \in U$. Now it is easy to see that $\phi_2 = \phi_1|_{G_2}$, so $\mathrm{Ker}\phi_2 = \mathrm{Ker}\phi_1 \cap G_2$. Now we need to show that $\mathrm{Ker}\phi_1 \subseteq G_2$. For this let $e_1, \ldots, e_m$ be a basis of U, then we can extend this to a basis $e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+n}$ of V. Now let $g \in \mathrm{Ker}\phi_1$, then

(i) Suppose $i, j \leq m$, then $ge_i = e_i$, $ge_j = e_j$. Thus $\xi(ge_i, ge_j) = \xi(e_i, e_j)$.

(ii) Suppose $i \leq m$ and $j > m$, then $ge_i = e_i$, $ge_j = e_j + u$ for some $u \in U$. Thus $\xi(ge_i, ge_j) = \xi(e_i, e_j + u) = \xi(e_i, e_j)$.

(iii) Suppose $j \leq m$ and $i > m$, then $ge_i = e_i + u$ for some $u \in U$, $ge_j = e_j$. Thus $\xi(ge_i, ge_j) = \xi(e_i + u, e_j) = \xi(e_i, e_j)$.

(iv) Suppose $i, j > m$, then $ge_i = e_i + u$, $ge_j = e_j + v$ for some $u, v \in U$. Thus $\xi(ge_i, ge_j) = \xi(e_i + u, e_j + v) = \xi(e_i, e_j)$.

□

Remark 4.6.4. If we replace $\mathrm{Aut}(V,\xi)$ by $\mathrm{Aut}(V,H)$ or by $\mathrm{Aut}(V,Q)$ in the above lemma, then it still holds.

4.7 Main results

Now we are in a position to solve our main problems.

Definition 4.7.1. Let B be a singular bilinear form on a vector space V over the field F_q. Let $U = \mathrm{Rad}B$, then we can define a bilinear form on V/U by $\bar{B}(\bar{v}, \bar{w}) = B(v, w)$. It is easy to see that $\bar{B}$ is well defined.

Theorem 4.7.2. *Suppose $G = \mathrm{Aut}(V,\xi)$ and $x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}$ is the dual basis of V^* corresponding to the basis $e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+n}$ of V. Let $S = F_q[x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}]$ and $U = \mathrm{Rad}\xi = \langle e_1, \ldots, e_m \rangle$. Then for $y_i = \prod_{x \in (V/U)^*} (x_i - x)$, we have $S^G \cong F_q[y_1, \ldots, y_m]^{GL(U)} \otimes F_q[x_{m+1}, \ldots, x_{m+n}]^{S_P(V/U,\, \bar{\xi})}$.*

Proof. Define a map $\phi : G \to GL(U) \times GL(V/U)$ by $\phi(g) = (g|_U, \bar{g})$ where $\bar{g}(v+U) = g(v) + U$, then ϕ is a homomorphism. Let $N = \mathrm{Ker}\phi$, then by the first Isomorphism Theorem, we have $G/N \cong \mathrm{Im}\phi$. Further, we have $\mathrm{Im}\phi = GL(U) \times S_P(V/U, \bar{\xi})$.

Therefore, $G/N \cong GL(U) \times S_P(V/U,\bar{\xi})$. From Lemma 4.6.3, we have $S^N = F_q[y_1,\ldots,y_m,x_{m+1},\ldots,x_{m+n}]$. So according to Lemma 4.1.2 and Lemma 4.2.4, we have $(S^N)^{G/N} \cong F_q[y_1,\ldots,y_m]^{GL(U)} \otimes F_q[x_{m+1},\ldots,x_{m+n}]^{S_p(V/U,\,\bar{\xi})}$. By applying Lemma 4.1.1, we get $S^G \cong F_q[y_1,\ldots,y_m]^{GL(U)} \otimes F_q[x_{m+1},\ldots,x_{m+n}]^{S_P(V/U,\,\bar{\xi})}$. □

Definition 4.7.3. Suppose H is a singular hermitian form on a vector space V over the finite field F_{q^2}. Let $U = \mathrm{Rad}H$, then we can define a hermitian form on V/U by $\bar{H}(\bar{v},\bar{w}) = H(v,w)$. It is easy to check that $\bar{H}$ is well defined.

Theorem 4.7.4. *Suppose $G = \mathrm{Aut}(V,H)$ and $x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+n}$ is the dual basis of V^* corresponding to the basis $e_1,\ldots,e_m,e_{m+1},\ldots,e_{m+n}$ of V. Let $S = F_{q^2}[x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+n}]$ and $W = \mathrm{Rad}H = \langle e_1,\ldots,e_m\rangle$. Then for $y_i = \prod_{x\in(V/W)^*}(x_i - x)$, we have $S^G \cong F_{q^2}[y_1,\ldots,y_m]^{GL(W)} \otimes F_{q^2}[x_{m+1},\ldots,x_{m+n}]^{U(V/W,\,\bar{H})}$.*

Proof. Define a map $\phi : G \to GL(W) \times GL(V/W)$ as in Theorem 4.7.2. Let $N = \mathrm{Ker}\phi$, then $G/N \cong \mathrm{Im}\phi$. Further, we have $\mathrm{Im}\phi = GL(W) \times U(V/W,\bar{H})$. Therefore, $G/N \cong GL(W) \times U(V/W,\bar{H})$. From Remark 4.6.4, we have $S^N = F_{q^2}[y_1,\ldots,y_m,x_{m+1},\ldots,x_{m+n}]$. By using Lemma 4.1.2 and Lemma 4.2.4, we have $(S^N)^{G/N} \cong F_{q^2}[y_1,\ldots,y_m]^{GL(W)} \otimes F_{q^2}[x_{m+1},\ldots,x_{m+n}]^{U(V/W,\,\bar{H})}$. So by Lemma 4.1.1, we get $S^G \cong F_{q^2}[y_1,\ldots,y_m]^{GL(W)} \otimes F_{q^2}[x_{m+1},\ldots,x_{m+n}]^{U(V/W,\,\bar{H})}$. □

Definition 4.7.5. Let Q be a singular quadratic form on a vector space V over the finite field F_q. Let $U = \mathrm{Rad}Q$. We can define a quadratic form on V/U by $\bar{Q}(\bar{v}) = Q(v)$. It is easy to check that $\bar{Q}$ is well defined.

Theorem 4.7.6. *Suppose $G = \mathrm{Aut}(V,Q)$ and $x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+n}$ is the dual basis of V^* corresponding to the basis $e_1,\ldots,e_m,e_{m+1},\ldots,e_{m+n}$ of V. Let $S = F_q[x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+n}]$ and $U = \mathrm{Rad}Q = \langle e_1,\ldots,e_m\rangle$. Then for $y_i = \prod_{x\in(V/U)^*}(x_i - x)$, we have $S^G \cong F_q[y_1,\ldots,y_m]^{GL(U)} \otimes F_q[x_{m+1},\ldots,x_{m+n}]^{O(V/U,\,\bar{Q})}$.*

Proof. Define a map $\phi : G \to GL(U) \times GL(V/U)$ as in the theorems above. Let $N = \mathrm{Ker}\phi$. Then since $\mathrm{Im}\phi = GL(U) \times O(V/U,\bar{Q})$ we have $G/N \cong GL(U) \times O(V/U,\bar{Q})$. By Remark 4.6.4, we have $S^N = F_q[y_1,\ldots,y_m,x_{m+1},\ldots,x_{m+n}]$. Therefore by Lemma 4.1.2 and Lemma 4.2.4, we have $(S^N)^{G/N} \cong F_q[y_1,\ldots,y_m]^{GL(U)} \otimes$

$F_q[x_{m+1},\ldots,x_{m+n}]^{O(V/U,\ \bar{Q})}$. Thus by Lemma 4.1.1, we get $S^G \cong F_q[y_1,\ldots,y_m]^{GL(U)} \otimes F_q[x_{m+1},\ldots,x_{m+n}]^{O(V/U,\ \bar{Q})}$. □

Remark 4.7.7. From Theorem 4.7.2 and Theorem 4.7.4 it is easy to see that S^G is a graded complete intersection, and so in particular it is Gorenstein and Cohen-Macaulay. But from Theorem 4.7.6 S^G is a graded complete intersection when the characteristic of the field F_q is odd or $q = 2$ as we do not know about

$$F_q[x_{m+1},\ldots,x_{m+n}]^{O(V/U,\ \bar{Q})} \text{ when } q = 2^l, l \geq 2.$$

Chapter 5

Invariant rings of subgroups of the symplectic group

Let V be a vector space over the field F_q. Suppose $e_1, \ldots, e_{2n}$ is a basis of V and U is a subspace of V. Let ξ be the non-degenerate alternating form on the vector space V with the following matrix:

$$\begin{bmatrix} 0 & 1 & & & & & & \\ -1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & & 0 & 1 \\ & & & & & & -1 & 0 \end{bmatrix}$$

filled out with zeroes.

In this chapter we want to find the invariant ring S^G where $S = F_q[V]$ and $G = \{g \in Sp(V, \xi) : gU = U\}$. We shall consider the following two cases:

(i) $U = \langle e_1, e_2, \ldots, e_m \rangle$ where m is even and less than $2n$;

(ii) $U = \langle e_1, e_3, \ldots, e_{2n-1} \rangle$.

5.1 The orthogonal complement and some related results

Definition 5.1.1. Let ξ be an alternating form on V. For a subspace U of V, we denote the *orthogonal complement* of U by $U^{\perp}$. This is defined as

$$U^{\perp} = \{v \in V : \xi(u, v) = 0 \ \forall \ u \in U\}.$$

Now let us present some nice properties of the orthogonal complement which are important.

Lemma 5.1.2. *Let V be a vector space over the field F_q and ξ be a non-degenerate alternating form on V. Suppose U is a subspace of V. If $\xi|_U$ is a non-degenerate alternating form on U, then*

(i) $V = U \oplus U^{\perp}$ and

(ii) $\xi|_{U^{\perp}}$ is a non-degenerate alternating form on $U^{\perp}$.

Proof. Follows from Theorem 11.8 in [35]. □

Lemma 5.1.3. *Let V be a vector space over the field F_q and ξ be a non-degenerate alternating form on V. Suppose U is a subspace of V, then $(U^{\perp})^{\perp} = U$.*

Proof. Follows from Theorem 11.7 in [35]. □

Theorem 5.1.4. *Let $H = \{g \in Sp(V, \xi) : gU^{\perp} = U^{\perp}\}$, then $H = G$.*

Proof. If $g \in G$ and $w \in U^{\perp}$, then we have $\xi(u, gw) = \xi(g^{-1}u, w) = 0$ for all $u \in U$. This implies that $gw \in U^{\perp}$. Conversely, suppose that $g \in H$ and $w \in U$, then $\xi(u, gw) = \xi(g^{-1}u, w) = 0$ for all $u \in U^{\perp}$. This implies that $gw \in (U^{\perp})^{\perp}$. Hence $gw \in U$ by Lemma 5.1.3. □

We now state a useful result which is called Witt's Lemma. Witt's Lemma is very important in invariant theory and we shall use this result in our later sections.

Theorem 5.1.5. *(Witt's Lemma on page 81 in [1]). Let V be an orthogonal, symplectic or unitary space. Let U and W be subspaces of V and suppose $\alpha : U \to W$ is an isometry. Then α extends to an isometry of V.*

5.2 Main result in the first case

Theorem 5.2.1. *Let $x_1, \ldots, x_{2n}$ be the dual basis of V^* corresponding to the basis $e_1, \ldots, e_{2n}$ of V. Suppose $S = F_q[x_1, \ldots, x_{2n}]$ and $U = \langle e_1, e_2, \ldots, e_m \rangle$ as defined on page 88. Then $S^G \cong F_q[x_1, x_2, \ldots, x_m]^{Sp(U,\ \xi|_U)} \otimes F_q[x_{m+1}, x_{m+2}, \ldots, x_{2n}]^{Sp(U^\perp,\ \xi|_{U^\perp})}$.*

Proof. First note that $\xi|_U$ is non-degenerate on U. Define a map $\phi : G \to GL(U) \times GL(U^\perp)$ by $\phi(g) = (g|_U, g|_{U^\perp})$ where $g|_U(u) = g(u)$ for all $u \in U$ and $g|_{U^\perp}(w) = g(w)$ for $w \in U^\perp$. We can check ϕ is a homomorphism. By Lemma 5.1.2 (i) ϕ is injective with $\mathrm{Im}\phi = Sp(U, \xi|_U) \times Sp(U^\perp, \xi|_{U^\perp})$. Thus we have $G \cong Sp(U, \xi|_U) \times Sp(U^\perp, \xi|_{U^\perp})$. Therefore by Lemma 4.1.2 and Lemma 4.2.4,

$$S^G \cong F_q[x_1, x_2, \ldots, x_m]^{Sp(U,\ \xi|_U)} \otimes F_q[x_{m+1}, x_{m+2}, \ldots, x_{2n}]^{Sp(U^\perp,\ \xi|_{U^\perp})}. \qquad \square$$

Remark 5.2.2. From the above theorem it is clear that S^G is a graded complete intersection, and so in particular it is Gorenstein and Cohen-Macaulay.

5.3 Research strategies for the second case

Consider $U = \langle e_1, e_3, \ldots, e_{2n-1} \rangle$. Here $\xi|_U$ is a degenerate alternating form on U and $U = U^\perp$. Define a homomorphism $\phi : G \to GL(U)$ by $\phi(g) = g|_U$. By Theorem 5.1.5 ϕ is onto. If $N = \mathrm{Ker}\phi = \{g \in G : g(u) = I(u)\ \forall\ u \in U\}$, then $G/N \cong GL(U)$. The matrix of N is

$$\begin{bmatrix}
1 & a_{12} & 0 & a_{14} & \cdots & a_{1\ 2n-2} & 0 & a_{1\ 2n} \\
0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & a_{32} & 1 & a_{34} & \cdots & a_{3\ 2n-2} & 0 & a_{3\ 2n} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & a_{2n-1\ 2} & 0 & a_{2n-1\ 4} & \cdots & a_{2n-1\ 2n-2} & 1 & a_{2n-1\ 2n} \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1
\end{bmatrix}$$

with $a_{32} = a_{14}, \ldots, a_{2n-1\ 2} = a_{1\ 2n},\ a_{54} = a_{36}, \ldots, a_{2n-1\ 4} = a_{3\ 2n}, \ldots, a_{2n-1\ 2n-2} = a_{2n-3\ 2n}$.

Let $g \in N$, then $x_2^g = x_2, \ldots, x_{2n}^g = x_{2n}$. Now $x_i^g = x_i +$ something in $(V/U)^*$ for all odd i in the range $1 \leq i \leq 2n-1$, where $(V/U)^* = \langle x_2, x_4, \ldots, x_{2n} \rangle$. Look at $y_i = \prod_{x \in (V/U)^*} (x_i - x) \in S^N$ for $i = 1, 3, \ldots, 2n-1$. Also $\xi_i \in S^N$ for $1 \leq i \leq n-1$. Let $R = F_q[y_1, y_3, \ldots, y_{2n-1}, x_2, x_4, \ldots, x_{2n}, \xi_1, \ldots, \xi_{n-1}]$, then $R \subseteq S^N \subseteq S$.

Before stating our next result it should be noted that it shall be convenient to use $c_{n,i}$ instead of $c_{V/U,i}$ in the following result and in the later section in this chapter.

Lemma 5.3.1. *The following $n-1$ relations hold in R:*

$$\xi_i^{q^{n-i}} + \sum_{j=1}^{n} x_{2j}^{q^{n-i}} y_{2j-1} + \sum_{j=1}^{n-i} (-1)^{j+i+1} c_{n,n-j-i} \xi_j^{q^{n-j-i}} + \sum_{j=1}^{i-1} (-1)^j c_{n,n-j} \xi_{i-j}^{q^{n-i}} = 0$$

where $1 \leq i \leq n-1$.

Proof. We start by proving the first relation. For simplicity suppose n is even. Since

$$\xi_i = x_1 x_2^{q^i} - x_2 x_1^{q^i} + \cdots + x_{2n-1} x_{2n}^{q^i} - x_{2n} x_{2n-1}^{q^i},$$

then

$$\xi_1^{q^{n-1}} = x_1^{q^{n-1}} x_2^{q^n} - x_2^{q^{n-1}} x_1^{q^n} + \cdots + x_{2n-1}^{q^{n-1}} x_{2n}^{q^{n-1}} - x_{2n}^{q^{n-1}} x_{2n-1}^{q^n}.$$

Also

$$y_i = x_i^{q^n} - c_{n,n-1} x_i^{q^{n-1}} + c_{n,n-2} x_i^{q^{n-2}} - \cdots - c_{n,1} x_i^q + c_{n,0} x_i.$$

Multiplying y_i by $x_{i+1}^{q^{n-1}}$ for odd i in the range $1 \leq i \leq 2n-1$ and adding $\xi_1^{q^{n-1}}$, we get

$$\begin{aligned}
&\xi_1^{q^{n-1}} + x_2^{q^{n-1}} y_1 + x_4^{q^{n-1}} y_3 + \cdots + x_{2n-2}^{q^{n-1}} y_{2n-3} + x_{2n}^{q^{n-1}} y_{2n-1} \\
&= x_1^{q^{n-1}} x_2^{q^n} + x_3^{q^{n-1}} x_4^{q^n} + \cdots + x_{2n-3}^{q^{n-1}} x_{2n-2}^{q^n} + x_{2n-1}^{q^{n-1}} x_{2n}^{q^n} - \\
&c_{n,n-1}(x_1^{q^{n-1}} x_2^{q^{n-1}} + x_3^{q^{n-1}} x_4^{q^{n-1}} + \cdots + x_{2n-3}^{q^{n-1}} x_{2n-2}^{q^{n-1}} + x_{2n-1}^{q^{n-1}} x_{2n}^{q^{n-1}}) + \\
&c_{n,n-2}(x_1^{q^{n-2}} x_2^{q^{n-1}} + x_3^{q^{n-2}} x_4^{q^{n-1}} + \cdots + x_{2n-3}^{q^{n-2}} x_{2n-2}^{q^{n-1}} + x_{2n-1}^{q^{n-2}} x_{2n}^{q^{n-1}}) - \\
&\cdots - c_{n,1}(x_1^q x_2^{q^{n-1}} + x_3^q x_4^{q^{n-1}} + \cdots + x_{2n-3}^q x_{2n-2}^{q^{n-1}} + x_{2n-1}^q x_{2n}^{q^{n-1}}) + \\
&c_{n,0}(x_1 x_2^{q^{n-1}} + x_3 x_4^{q^{n-1}} + \cdots + x_{2n-3} x_{2n-2}^{q^{n-1}} + x_{2n-1} x_{2n}^{q^{n-1}}).
\end{aligned}$$

Thus, we have

$$\xi_1^{q^{n-1}}+x_2^{q^{n-1}}y_1+x_4^{q^{n-1}}y_3+\cdots+x_{2n-2}^{q^{n-1}}y_{2n-3}+x_{2n}^{q^{n-1}}y_{2n-1}-c_{n,n-2}\xi_1^{q^{n-2}}+\cdots+c_{n,1}\xi_{n-2}^{q}-c_{n,0}\xi_{n-1}$$

$$= x_1^{q^{n-1}}x_2^{q^n}+x_3^{q^{n-1}}x_4^{q^n}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q^n}+x_{2n-1}^{q^{n-1}}x_{2n}^{q^n}-$$

$$c_{n,n-1}(x_1^{q^{n-1}}x_2^{q^{n-1}}+x_3^{q^{n-1}}x_4^{q^{n-1}}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q^{n-1}}+x_{2n-1}^{q^{n-1}}x_{2n}^{q^{n-1}})+$$

$$c_{n,n-2}(x_1^{q^{n-1}}x_2^{q^{n-2}}+x_3^{q^{n-1}}x_4^{q^{n-2}}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q^{n-2}}+x_{2n-1}^{q^{n-1}}x_{2n}^{q^{n-2}})-$$

$$\cdots-c_{n,1}(x_1^{q^{n-1}}x_2^{q}+x_3^{q^{n-1}}x_4^{q}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q}+x_{2n-1}^{q^{n-1}}x_{2n}^{q})+$$

$$c_{n,0}(x_1^{q^{n-1}}x_2+x_3^{q^{n-1}}x_4+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}+x_{2n-1}^{q^{n-1}}x_{2n}).$$

Hence we need to show that

$$\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} (x_1^{q^{n-1}}x_2^{q^n}+x_3^{q^{n-1}}x_4^{q^n}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q^n}+x_{2n-1}^{q^{n-1}}x_{2n}^{q^n})$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n}} & x_4^{q^{n}} & \cdots & x_{2n-2}^{q^{n}} & x_{2n}^{q^{n}} \end{vmatrix} (x_1^{q^{n-1}}x_2^{q^{n-1}}+x_3^{q^{n-1}}x_4^{q^{n-1}}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q^{n-1}}+x_{2n-1}^{q^{n-1}}x_{2n}^{q^{n-1}})$$

$$+\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^{n}} & x_4^{q^{n}} & \cdots & x_{2n-2}^{q^{n}} & x_{2n}^{q^{n}} \end{vmatrix} (x_1^{q^{n-1}}x_2^{q^{n-2}}+x_3^{q^{n-1}}x_4^{q^{n-2}}+\cdots+x_{2n-3}^{q^{n-1}}x_{2n-2}^{q^{n-2}}+x_{2n-1}^{q^{n-1}}x_{2n}^{q^{n-2}})$$

$$
\begin{aligned}
&-\dots\\
&-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^{q^{n-1}}x_2^q + x_3^{q^{n-1}}x_4^q + \cdots + x_{2n-3}^{q^{n-1}}x_{2n-2}^q + x_{2n-1}^{q^{n-1}}x_{2n}^q)\\
&+\begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^{q^{n-1}}x_2 + x_3^{q^{n-1}}x_4 + \cdots + x_{2n-3}^{q^{n-1}}x_{2n-2} + x_{2n-1}^{q^{n-1}}x_{2n})\\
&= 0.
\end{aligned}
$$

Now L.H.S =

$$
\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_1^{q^{n-1}}x_2^{q^n}
$$

$$
-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^{q^{n-1}}x_2^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^{q^{n-1}}x_2^{q^{n-2}}
$$

$$
\begin{aligned}
&-\dots\\
&-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^{q^{n-1}}x_2^q + \begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^{q^{n-1}}x_2
\end{aligned}
$$

$$+\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_3^{q^{n-1}} x_4^{q^n}$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^{q^{n-1}} x_4^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^{q^{n-1}} x_4^{q^{n-2}}$$

$$-\ldots$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^{q^{n-1}} x_4^q + \begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^{q^{n-1}} x_4$$

$$+\ldots$$

$$+\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_{2n-3}^{q^{n-1}} x_{2n-2}^{q^n}$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^{q^{n-1}} x_{2n-2}^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^{q^{n-1}} x_{2n-2}^{q^{n-2}}$$

$$-\dots$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^{q^{n-1}} x_{2n-2}^{q} + \begin{vmatrix} x_2^{q} & x_4^{q} & \cdots & x_{2n-2}^{q} & x_{2n}^{q} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^{q^{n-1}} x_{2n-2}$$

$$+\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q} & x_4^{q} & \cdots & x_{2n-2}^{q} & x_{2n}^{q} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_{2n-1}^{q^{n-1}} x_{2n}^{q^n}$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q} & x_4^{q} & \cdots & x_{2n-2}^{q} & x_{2n}^{q} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^{q^{n-1}} x_{2n}^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^{q^{n-1}} x_{2n}^{q^{n-2}}$$

$$-\dots$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^{q^{n-1}} x_{2n}^{q} + \begin{vmatrix} x_2^{q} & x_4^{q} & \cdots & x_{2n-2}^{q} & x_{2n}^{q} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^{q^{n-1}} x_{2n}.$$

Thus by expanding each determinant of L.H.S by the first column in part one, by the second column in part two and so on, we shall get 0. In the same way we can do this when n is odd.

Now we prove the last relation. For simplicity suppose n is odd, then

$$y_i = x_i^{q^n} - c_{n,n-1}x_i^{q^{n-1}} + c_{n,n-2}x_i^{q^{n-2}} - \cdots + c_{n,1}x_i^{q} - c_{n,0}x_i.$$

Now

$$\xi_{n-1}^q = x_1^q x_2^{q^n} - x_2^q x_1^{q^n} + \cdots + x_{2n-1}^q x_{2n}^{q^n} - x_{2n}^q x_{2n-1}^{q^n}.$$

Multiplying y_i by x_{i+1}^q for odd i in the range $1 \leq i \leq 2n-1$ and adding ξ_{n-1}^q, we get

$$\begin{gathered}
\xi_{n-1}^q + x_2^q y_1 + x_4^q y_3 + \cdots + x_{2n-2}^q y_{2n-3} + x_{2n}^q y_{2n-1} \\
= x_1^q x_2^{q^n} + x_3^q x_4^{q^n} + \cdots + x_{2n-3}^q x_{2n-2}^{q^n} + x_{2n-1}^q x_{2n}^{q^n} - \\
c_{n,n-1}(x_1^{q^{n-1}} x_2^q + x_3^{q^{n-1}} x_4^q + \cdots + x_{2n-3}^{q^{n-1}} x_{2n-2}^q + x_{2n-1}^{q^{n-1}} x_{2n}^q) + \\
c_{n,n-2}(x_1^{q^{n-2}} x_2^q + x_3^{q^{n-2}} x_4^q + \cdots + x_{2n-3}^{q^{n-2}} x_{2n-2}^q + x_{2n-1}^{q^{n-2}} x_{2n}^q) - \\
\cdots - c_{n,2}(x_1^{q^2} x_2^q + x_3^{q^2} x_4^q + \cdots + x_{2n-3}^{q^2} x_{2n-2}^q + x_{2n-1}^{q^2} x_{2n}^q) + \\
c_{n,1}(x_1^q x_2^q + x_3^q x_4^q + \cdots + x_{2n-3}^q x_{2n-2}^q + x_{2n-1}^q x_{2n}^q) - \\
c_{n,0}(x_1 x_2^q + x_3 x_4^q + \cdots + x_{2n-3} x_{2n-2}^q + x_{2n-1} x_{2n}^q).
\end{gathered}$$

Thus, we have

$$\begin{gathered}
\xi_{n-1}^q + x_2^q y_1 + x_4^q y_3 + \cdots + x_{2n-2}^q y_{2n-3} + x_{2n}^q y_{2n-1} - c_{n,n-1}\xi_{n-2}^q + c_{n,n-2}\xi_{n-3}^q - \cdots - c_{n,2}\xi_1^q + c_{n,0}\xi_1 \\
= x_1^q x_2^{q^n} + x_3^q x_4^{q^n} + \cdots + x_{2n-3}^q x_{2n-2}^{q^n} + x_{2n-1}^q x_{2n}^{q^n} - \\
c_{n,n-1}(x_1^q x_2^{q^{n-1}} + x_3^q x_4^{q^{n-1}} + \cdots + x_{2n-3}^q x_{2n-2}^{q^{n-1}} + x_{2n-1}^q x_{2n}^{q^{n-1}}) + \\
c_{n,n-2}(x_1^q x_2^{q^{n-2}} + x_3^q x_4^{q^{n-2}} + \cdots + x_{2n-3}^q x_{2n-2}^{q^{n-2}} + x_{2n-1}^q x_{2n}^{q^{n-2}}) - \\
\cdots - c_{n,2}(x_1^q x_2^{q^2} + x_3^q x_4^{q^2} + \cdots + x_{2n-3}^q x_{2n-2}^{q^2} + x_{2n-1}^q x_{2n}^{q^2}) + \\
c_{n,1}(x_1^q x_2^q + x_3^q x_4^q + \cdots + x_{2n-3}^q x_{2n-2}^q + x_{2n-1}^q x_{2n}^q) - \\
c_{n,0}(x_1^q x_2 + x_3^q x_4 + \cdots + x_{2n-3}^q x_{2n-2} + x_{2n-1}^q x_{2n}).
\end{gathered}$$

Hence, we need to show that

$$\begin{vmatrix}
x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\
x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\
x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}}
\end{vmatrix} (x_1^q x_2^{q^n} + x_3^q x_4^{q^n} + \cdots + x_{2n-3}^q x_{2n-2}^{q^n} + x_{2n-1}^q x_{2n}^{q^n})$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^q x_2^{q^{n-1}} + x_3^q x_4^{q^{n-1}} + \cdots + x_{2n-3}^q x_{2n-2}^{q^{n-1}} + x_{2n-1}^q x_{2n}^{q^{n-1}})$$

$$+\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^q x_2^{q^{n-2}} + x_3^q x_4^{q^{n-2}} + \cdots + x_{2n-3}^q x_{2n-2}^{q^{n-2}} + x_{2n-1}^q x_{2n}^{q^{n-2}})$$

$-\ldots$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^3} & x_4^{q^3} & \cdots & x_{2n-2}^{q^3} & x_{2n}^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^q x_2^{q^2} + x_3^q x_4^{q^2} + \cdots + x_{2n-3}^q x_{2n-2}^{q^2} + x_{2n-1}^q x_{2n}^{q^2})$$

$$+\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^q x_2^q + x_3^q x_4^q + \cdots + x_{2n-3}^q x_{2n-2}^q + x_{2n-1}^q x_{2n}^q)$$

$$-\begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} (x_1^q x_2 + x_3^q x_4 + \cdots + x_{2n-3}^q x_{2n-2} + x_{2n-1}^q x_{2n})$$

$= 0.$

Now L.H.S =

$$\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_1^q x_2^{q^n}$$

$$- \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^q x_2^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^q x_2^{q^{n-2}}$$

$$- \cdots$$

$$- \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^3} & x_4^{q^3} & \cdots & x_{2n-2}^{q^3} & x_{2n}^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^q x_2^{q^2} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^q x_2^q$$

$$- \begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_1^q x_2 + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-1}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_3^q x_4^{q^n}$$

$$- \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^q x_4^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^q x_4^{q^{n-2}}$$

$$-\dots$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^3} & x_4^{q^3} & \cdots & x_{2n-2}^{q^3} & x_{2n}^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^q x_4^{q^2} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^q x_4^q$$

$$-\begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_3^q x_4 + \cdots + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_{2n-3}^q x_{2n-2}^{q^n}$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^q x_{2n-2}^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^q x_{2n-2}^{q^{n-2}}$$

$$-\dots$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^3} & x_4^{q^3} & \cdots & x_{2n-2}^{q^3} & x_{2n}^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^q x_{2n-2}^{q^2} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^q x_{2n-2}^q$$

$$-\begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-3}^q x_{2n-2} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \end{vmatrix} x_{2n-1}^q x_{2n}^{q^n}$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-2}} & x_4^{q^{n-2}} & \cdots & x_{2n-2}^{q^{n-2}} & x_{2n}^{q^{n-2}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^q x_{2n}^{q^{n-1}} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-3}} & x_4^{q^{n-3}} & \cdots & x_{2n-2}^{q^{n-3}} & x_{2n}^{q^{n-3}} \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^q x_{2n}^{q^{n-2}}$$

$$-\ldots$$

$$-\begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^3} & x_4^{q^3} & \cdots & x_{2n-2}^{q^3} & x_{2n}^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^q x_{2n}^{q^2} + \begin{vmatrix} x_2 & x_4 & \cdots & x_{2n-2} & x_{2n} \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^q x_{2n}^q$$

$$-\begin{vmatrix} x_2^q & x_4^q & \cdots & x_{2n-2}^q & x_{2n}^q \\ x_2^{q^2} & x_4^{q^2} & \cdots & x_{2n-2}^{q^2} & x_{2n}^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2^{q^{n-1}} & x_4^{q^{n-1}} & \cdots & x_{2n-2}^{q^{n-1}} & x_{2n}^{q^{n-1}} \\ x_2^{q^n} & x_4^{q^n} & \cdots & x_{2n-2}^{q^n} & x_{2n}^{q^n} \end{vmatrix} x_{2n-1}^q x_{2n}.$$

Thus by expanding each determinant of L.H.S by the first column in part one, by the second column in part two and so on, we shall get 0. In the same way we can do this when n is even. □

Similarly, we can verify the rest of the relations.

5.4 The Computation of the invariant ring S^N

Let $S = F_q[x_1, \ldots, x_{2n}]$ and $N = \{g \in G : g(u) = u \ \forall \ u \in U\}$ as defined on page 90. In this section we show that the generators and relators found above give a presentation of S^N. Before doing this we discuss an earlier failed attempt at a proof. Our earlier attempt worked in dimension 4 but failed in dimension 6. The investigation is described in the following results. The reader interested only in the

general case may skip Theorem 5.4.3, Theorem 5.4.4 and Remark 5.4.5. The next two results formed a part of our failed proof but are also essential for establishing the presentation in general.

Lemma 5.4.1. *Let* $R = F_q[y_1, y_3, \ldots, y_{2n-1}, x_2, \ldots, x_{2n}, \xi_1, \ldots, \xi_{n-1}]$ *and* $S = F_q[x_1, \ldots, x_{2n}]$. *Then* S *is integral over* R.

Proof. For $x_i \in S$, where $i = 2, 4, \ldots, 2n$, there exist polynomials $P_i(X) = X - x_i \in R[X]$ such that $P_i(x_i) = 0$. Also for $x_j \in S$, where $j = 1, 3, \ldots, 2n-1$, there exist polynomials $P_j(X) = D_{(V/U)}(X - x_j) \in R[X]$ such that $P_j(x_j) = 0$. □

Theorem 5.4.2. *Let* $R = F_q[y_1, y_3, \ldots, y_{2n-1}, x_2, \ldots, x_{2n}, \xi_1, \ldots, \xi_{n-1}]$ *and* $S = F_q[x_1, \ldots, x_{2n}]$, *then* $ff(R) = ff(S^N)$.

Proof. Since $R \subseteq S^N \subseteq S$, then obviously $ff(R) \subseteq ff(S^N)$. Thus we need to show that $ff(S^N) \subseteq ff(R)$. For this we need to check that $ff(R) \subseteq ff(S)$ is a finite separable normal field extension. The polynomials $P_j(X) = \underset{(V/U)}{D}(X - x_j)$ for $j = 1, 3, \ldots, 2n-1$ split over $ff(S)$, where $P_j(X) \in R[X]$, and it is easy to see that $ff(S) = ff(R)(x_1, x_3, \ldots, x_{2n-1})$. Thus by definition $ff(S)$ is the splitting field for these polynomials and so by Theorem 4.3.4 the extension $ff(R) \subseteq ff(S)$ is finite and normal. Now the elements $x_1, x_3, \ldots, x_{2n-1}$ are separable. Therefore by Theorem 4.3.7 the extension $ff(R) \subseteq ff(S)$ is separable. Let H be the Galois group of the field extension $ff(R) \subseteq ff(S)$. On the other hand Proposition 4.3.13 shows that the field extension $ff(S^N) \subseteq ff(S)$ is Galois with Galois group N. Thus by Theorem 4.3.12 $N \subseteq H$. Let $R' = F_q[y_1, \ldots, y_{2n-1}, x_2, \ldots, x_{2n}]$ and H' be the Galois group of the field extension $ff(R') \subseteq ff(S)$. If we take $U = \langle e_1, e_3, \ldots, e_{2n-1} \rangle$ and $G' = \{g \in GL(V) : gU = U\}$, then from section 4.6 part (ii) we have $H' = \{g \in G' : gu = u \ \forall \ u \in U$ and $gv - v \in U \ \forall \ v \in V\}$. By Theorem 4.3.12 $H \subseteq H'$. On the other hand $\xi_1^h = \xi_1$ for all $h \in H$. Thus by Lemma 2.2.3 it follows that $H \subseteq N$. Therefore $H = N$ and so by Theorem 4.3.12 $ff(R) = ff(S^N)$. □

Our first attempt to establish the presentation applied to the case $n = 2$.

Theorem 5.4.3. *Let $S = F_q[x_1, x_2, x_3, x_4]$ where x_1, x_2, x_3, x_4 is the dual basis of V^* corresponding to the basis e_1, e_2, e_3, e_4 of V. If $R = F_q[y_1, y_3, x_2, x_4, \xi_1]$, then R is integrally closed.*

Proof. We introduce formal variables $Y_1, Y_3, X_2, X_4, \Xi_1$ and define a map

$$\phi : T = F_q[Y_1, Y_3, X_2, X_4, \Xi_1] \to R$$

by sending Y_i to y_i, X_i to x_i and Ξ_1 to ξ_1. Obviously this is an epimorphism and so $T/\mathrm{Ker}\phi \cong R$. Let

$$\rho = \Xi_1^q - \Xi_1 C_{2,0} + Y_1 X_2^q + Y_3 X_4^q. \tag{5.1}$$

Now $T/\mathrm{Ker}\phi$ is an integral domain and $T/\mathrm{Ker}\phi \subseteq S$. Thus by Lemma 4.4.4 $\dim(T/\mathrm{Ker}\phi) \leq 4$. Let $R' = F_q[y_1, y_3, x_2, x_4]$. Now the polynomials $P_j(X) = \underset{(V/U)}{D}(X - x_j)$ for $j = 1, 3$ split over $ff(S)$, where $P_j(X) \in R'[X]$, and it is easy to see that $ff(S) = ff(R')(x_1, x_3)$. Thus by definition $ff(S)$ is the splitting field for these polynomials and so by Theorem 4.3.4 the extension $ff(R') \subseteq ff(S)$ is finite and normal. Now the elements x_1, x_3 are separable. Therefore by Theorem 4.3.7 the extension $ff(R') \subseteq ff(S)$ is separable. Since the extension $ff(R') \subseteq ff(S)$ is finite and separable, so by the remark after Proposition 4.4.5 we have that y_1, y_3, x_2, x_4 are algebraically independent. Since $R' \subseteq T/\mathrm{Ker}\phi$, therefore again by Lemma 4.4.4 $\dim(T/\mathrm{Ker}\phi) \geq 4$. It follows that $\dim(T/\mathrm{Ker}\phi) = 4$. Note that $\langle\rho\rangle \subseteq \mathrm{Ker}\phi$. We need to show that $\mathrm{Ker}\phi = \langle\rho\rangle$. By Proposition 3.5.7, $\mathrm{htKer}\phi = 1$, so by Lemma 3.5.6 $\mathrm{Ker}\phi$ is a principal ideal. Also ρ is irreducible because if we consider it as a polynomial in Y_1, it is linear in Y_1 and the coefficient X_2^q of Y_1 does not divide all the other terms. Therefore, we have $\mathrm{Ker}\phi = \langle\rho\rangle$. Let $X_4 + \langle\rho\rangle = \hat{X_4}$ and consider the localization $T/\langle\rho\rangle[\hat{X_4}^{-1}]$ of $T/\langle\rho\rangle$. Then

$$T/\langle\rho\rangle[\hat{X_4}^{-1}] = F_q[\hat{Y_1}, \hat{X_2}, \hat{X_4}, \hat{X_4}^{-1}, \hat{\Xi_1}]$$

as the relation ρ enables us to express $\hat{Y_3}$ in terms of $\hat{Y_1}, \hat{X_2}, \hat{X_4}, \hat{\Xi_1}$ and $\hat{X_4}^{-1}$ and so eliminate $\hat{Y_3}$ from the generators of the ring. Note that the images of

$Y_1, X_2, X_4,$ and Ξ_1 in $T/\langle\rho\rangle$ are algebraically independent as the only relations imposed on $T/\langle\rho\rangle$ are multiples of ρ. Hence the sub-algebra L of $T/\langle\rho\rangle$ generated by the images of $Y_1, X_2, X_4,$ and Ξ_1 is a polynomial algebra. But

$$L[\hat{X_4}^{-1}] = T/\langle\rho\rangle[\hat{X_4}^{-1}].$$

Thus we see that $T/\langle\rho\rangle[\hat{X_4}^{-1}]$ is a UFD, being a localization of a polynomial ring . We observe that

$$T/\langle\rho\rangle/\langle\hat{X_4}\rangle \cong T/\langle X_4, \rho\rangle$$

$$= F_q[Y_1, Y_3, X_2, X_4, \Xi_1]/\langle X_4, \rho\rangle$$

$$\cong F_q[Y_1, Y_3, X_2, \Xi_1]/\langle \Xi_1^q + Y_1 X_2^q\rangle$$

where $\rho_0 = \Xi_1^q + Y_1 X_2^q$ is irreducible since ρ_0 is linear in Y_1 and the coefficient X_2^q of Y_1 does not divide the other term Ξ_1^q. Now since $F_q[Y_1, Y_3, X_4, \Xi_1]$ is a UFD, by Lemma 3.4.6, ρ_0 is prime. Therefore $F_q[Y_1, Y_3, X_2, \Xi_1]/\langle \Xi_1^q + Y_1 X_2^q\rangle$ is an integral domain and so by Lemma 3.4.8 $T/\langle\rho\rangle$ is a UFD. This completes the proof. □

Theorem 5.4.4. *Let $S = F_q[x_1, x_2, x_3, x_4]$ as in the above lemma, then $S^N = F_q[y_1, y_3, x_2, x_4, \xi_1]$.*

Proof. Follows from Lemma 5.4.1, Theorem 5.4.2, Theorem 5.4.3 and Lemma 4.2.2. □

This completes the proof when $n = 2$ but does not solve the problem when $n = 3$

Remark 5.4.5. The case $n = 3$. Let $S = F_q[x_1, x_2, x_3, x_4, x_5, x_6]$ where $x_1, x_2, x_3, x_4, x_5,$ x_6 is the dual basis of V^* corresponding to the basis $e_1, e_2, e_3, e_4, e_5, e_6$ of V. Let $R = F_q[y_1, y_3, y_5, x_2, x_4, x_6, \xi_1, \xi_2]$. We are going to show that the method used in Theorem 5.4.3 to show that R is integrally closed does not work here. We introduce formal variables $Y_1, Y_3, Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2$ and define a map

$$\phi : T = F_q[Y_1, Y_3, Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2] \to R$$

by sending Y_i to y_i, X_i to x_i and Ξ_i to ξ_i. Obviously this is an epimorphism and so $T/\mathrm{Ker}\phi \cong R$. Let

$$\rho_1 = \Xi_1^{q^2} + X_2^{q^2} Y_1 + X_4^{q^2} Y_3 + X_6^{q^2} Y_5 + C_{3,0}\Xi_2 - C_{3,1}\Xi_1^q \tag{5.2}$$

and

$$\rho_2 = \Xi_2^q + X_2^q Y_1 + X_4^q Y_3 + X_6^q Y_5 + C_{3,0}\Xi_1 - C_{3,2}\Xi_1^q. \tag{5.3}$$

We need to show that $\mathrm{Ker}\phi = \langle \rho_1, \rho_2 \rangle$. Since $\langle \rho_1, \rho_2 \rangle \subseteq \mathrm{Ker}\phi$, we have

$$W = T/\langle \rho_1, \rho_2 \rangle \overset{\psi}{\twoheadrightarrow} T/\mathrm{Ker}\phi \subseteq S^N.$$

Now $T/\mathrm{Ker}\phi$ is an integral domain and it has Krull dimension 6. We would like to prove that W is an integral domain of Krull dimension 6. Note that ρ_1 and ρ_2 can be written as:

$$\rho_1 \equiv \Xi_1^{q^2} \bmod \langle X_2, X_4, X_6 \rangle$$

and

$$\rho_2 \equiv \Xi_2^q \bmod \langle Y_1, Y_3, Y_5, \Xi_1 \rangle.$$

It follows that ρ_1, ρ_2 is a regular sequence. Thus by Theorem 3.7.13 $\dim W = 6$. Equation(5.2) and Equation(5.3) can be written in matrix form as follows:

$$\begin{bmatrix} \hat{X}_2^{q^2} & \hat{X}_4^{q^2} \\ \hat{X}_2^q & \hat{X}_4^q \end{bmatrix} \begin{bmatrix} \hat{Y}_1 \\ \hat{Y}_3 \end{bmatrix} = \begin{bmatrix} -\hat{\Xi}_1^{q^2} - \hat{X}_6^{q^2}\hat{Y}_5 - \hat{C}_{3,0}\hat{\Xi}_2 + \hat{C}_{3,1}\hat{\Xi}_1^q \\ -\hat{\Xi}_2^q - \hat{X}_6^q\hat{Y}_5 - \hat{C}_{3,0}\hat{\Xi}_1 + \hat{C}_{3,2}\hat{\Xi}_1^q \end{bmatrix}.$$

Let

$$\Delta = \begin{bmatrix} X_2^{q^2} & X_4^{q^2} \\ X_2^q & X_4^q \end{bmatrix} \text{ and let } \delta = |\Delta|.$$

Since X_2, X_6, Ξ_1, Ξ_2 and X_4, X_6, Ξ_1, Ξ_2 are regular sequences, by Theorem 3.6.3 and Lemma 3.6.6 $X_2^{q^2} X_4^q, X_6, \Xi_1^{q^2}, \Xi_2^q$ is a regular sequence. Thus by Lemma 3.6.4 and Lemma 3.6.5 it follows that ρ_1, ρ_2, δ is a regular sequence. To show that W is an integral domain we need to show that the localization $W[\hat{\delta}^{-1}]$ is an integral domain. Now

$$W[\hat{\delta}^{-1}] = F_q[\hat{Y_5}, \hat{X_2}, \hat{X_4}, \hat{X_6}, \hat{\Xi_1}, \hat{\Xi_2}, \hat{\delta}^{-1}]$$

since ρ_1 and ρ_2 enable us to express $\hat{Y_1}$ and $\hat{Y_3}$ in terms of $\hat{Y_5}, \hat{X_2}, \hat{X_4}, \hat{X_6}, \hat{\Xi_1}, \hat{\Xi_2}, \hat{\delta}^{-1}$ and so eliminate $\hat{Y_1}$ and $\hat{Y_3}$ from the generators of the ring. Note that the images of $Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2$ in W are algebraically independent. Hence the sub-algebra U generated by the images of $Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2$ is a polynomial algebra. But

$U[\hat{\delta}^{-1}] = W[\hat{\delta}^{-1}]$. Thus we see that $W[\hat{\delta}^{-1}]$ is a UFD, being a localization of a polynomial ring. In particular, W is an integral domain. Thus we deduce that ψ is an isomorphism. To prove W is integrally closed we would like to know that $\hat{\delta}$ generates a prime ideal in W. That is, we want to prove that $T/\langle \rho_1, \rho_2, \delta \rangle$ is an integral domain. From Equation(5.2) and Equation(5.3), we get

$(X_2^{q^2}\Xi_2^q - X_2^q\Xi_1^{q^2} + X_2^{q^2}C_{3,0}\Xi_1 - X_2^qC_{3,0}\Xi_2 - X_2^{q^2}C_{3,2}\Xi_1^q + X_2^qC_{3,1}\Xi_1^q) + \langle \rho_1, \rho_2, \delta \rangle$
$= (X_2^qX_6^{q^2} - X_2^{q^2}X_6^q)Y_5 + \langle \rho_1, \rho_2, \delta \rangle$.

Let $\delta' = X_2^qX_6^{q^2} - X_2^{q^2}X_6^q$. If $\rho_1, \rho_2, \delta, \delta'$ is a regular sequence and if the images of $Y_3, X_2, X_4, X_6, \Xi_1, \Xi_2$ in $T/\langle \rho_1, \rho_2, \delta \rangle$ are algebraically independent then $T/\langle \rho_1, \rho_2, \delta \rangle$ is an integral domain by the argument above. But $\rho_1, \rho_2, \delta, \delta'$ is not a regular sequence because X_2 appears in both δ and δ', and the images of $Y_3, X_2, X_4, X_6, \Xi_1, \Xi_2$ in $T/\langle \rho_1, \rho_2, \delta \rangle$ are not algebraically independent because $\delta = X_2^{q^2}X_4^q - X_2^qX_4^{q^2}$ and so $\hat{X}_2^{q^2}\hat{X}_4^q - \hat{X}_2^q\hat{X}_4^{q^2} = \langle \rho_1, \rho_2, \delta \rangle$. Thus our method fails here.

Similarly if we consider

$$\Delta = \begin{bmatrix} X_2^{q^2} & X_6^{q^2} \\ X_2^q & X_6^q \end{bmatrix} \text{ or } \Delta = \begin{bmatrix} X_4^{q^2} & X_6^{q^2} \\ X_4^q & X_6^q \end{bmatrix}.$$

Then $\delta = X_2^{q^2}X_6^q - X_2^qX_6^{q^2}$ or $\delta = X_4^{q^2}X_6^q - X_4^qX_6^{q^2}$. In both cases we can show that ρ_1, ρ_2, δ is a regular sequence. If $\delta = X_2^{q^2}X_6^q - X_2^qX_6^{q^2}$, then from Equation(5.2) and Equation(5.3) we get $\delta' = X_4^{q^2}X_6^q - X_4^qX_6^{q^2}$ but since X_6 appears in both δ and δ', we see that $\rho_1, \rho_2, \delta, \delta'$ is not a regular sequence. Also the images of $Y_1, X_2, X_4, X_6, \Xi_1, \Xi_2$ in $T/\langle \rho_1, \rho_2, \delta \rangle$ are not algebraically independent because $\delta = X_2^{q^2}X_6^q - X_2^qX_6^{q^2}$ and so $\hat{X}_2^{q^2}\hat{X}_6^q - \hat{X}_2^q\hat{X}_6^{q^2} = \langle \rho_1, \rho_2, \delta \rangle$. Now if $\delta = X_4^{q^2}X_6^q - X_4^qX_6^{q^2}$, then from Equation(5.2) and Equation(5.3) we get $\delta' = X_2^qX_4^{q^2} - X_2^{q^2}X_4^q$ but since X_4 appears in both δ and δ', we see that $\rho_1, \rho_2, \delta, \delta'$ is not a regular sequence. Also the images of $Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2$ in $T/\langle \rho_1, \rho_2, \delta \rangle$ are not algebraically independent because $\delta = X_4^{q^2}X_6^q - X_4^qX_6^{q^2}$ and so $\hat{X}_4^{q^2}\hat{X}_6^q - \hat{X}_4^q\hat{X}_6^{q^2} = \langle \rho_1, \rho_2, \delta \rangle$.

Now if we insert one more generator ξ_3 into R, then

$$R = F_q[y_1, y_3, y_5, x_2, x_4, x_6, \xi_1, \xi_2, \xi_3].$$

We get one more relation which is as follows:

$$\xi_3 + x_2y_1 + x_4y_3 + x_6y_5 + c_{3,1}\xi_1 - c_{3,2}\xi_2 = 0.$$

In the same way we introduce formal variables $Y_1, Y_3, Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2, \Xi_3$ and define a map

$$\phi : T = F_q[Y_1, Y_3, Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2, \Xi_3] \to R$$

by sending Y_i to y_i, X_i to x_i and Ξ_i to ξ_i. Obviously this is an epimorphism and so $T/\text{Ker}\phi \cong R$. Let

$$\rho_3 = \Xi_3 + X_2Y_1 + X_4Y_3 + X_6Y_5 + C_{3,1}\Xi_1 - C_{3,2}\Xi_2. \tag{5.4}$$

We need to show that $\text{Ker}\phi = \langle \rho_1, \rho_2, \rho_3 \rangle$. Since $\langle \rho_1, \rho_2, \rho_3 \rangle \subseteq \text{Ker}\phi$, so we have

$$W = T/\langle \rho_1, \rho_2, \rho_3 \rangle \overset{\psi}{\twoheadrightarrow} T/\text{Ker}\phi \subseteq S^N.$$

Now $T/\text{Ker}\phi$ is an integral domain and it has Krull dimension 6. We would like to prove that W is an integral domain of Krull dimension 6. For this ρ_3 can be written as

$$\rho_3 \equiv \Xi_3 \bmod \langle Y_1, Y_3, Y_5, \Xi_1, \Xi_2 \rangle.$$

Thus it follows that ρ_1, ρ_2, ρ_3 is a regular sequence. So by Theorem 3.7.13 $\dim W = 6$. Equation(5.2), Equation(5.3) and Equation(5.4) can be written in matrix form as follows:

$$\begin{bmatrix} \hat{X}_2^{q^2} & \hat{X}_4^{q^2} & \hat{X}_6^{q^2} \\ \hat{X}_2^{q} & \hat{X}_4^{q} & \hat{X}_6^{q} \\ \hat{X}_2 & \hat{X}_4 & \hat{X}_6 \end{bmatrix} \begin{bmatrix} \hat{Y}_1 \\ \hat{Y}_3 \\ \hat{Y}_5 \end{bmatrix} = \begin{bmatrix} -\hat{\Xi}_1^{q^2} - \hat{C}_{3,0}\hat{\Xi}_2 + \hat{C}_{3,1}\hat{\Xi}_1^{q} \\ -\hat{\Xi}_2^{q} - \hat{C}_{3,0}\hat{\Xi}_1 + \hat{C}_{3,2}\hat{\Xi}_1^{q} \\ -\hat{\Xi}_3 - \hat{C}_{3,1}\hat{\Xi}_1 + \hat{C}_{3,2}\hat{\Xi}_2 \end{bmatrix}.$$

Suppose

$$\Delta = \begin{bmatrix} X_2^{q^2} & X_4^{q^2} & X_6^{q^2} \\ X_2^{q} & X_4^{q} & X_6^{q} \\ X_2 & X_4 & X_6 \end{bmatrix} \text{ and let } \delta = |\Delta|.$$

By Theorem 3.6.3, Lemma 3.6.4, Lemma 3.6.5 and Lemma 3.6.6 we see that ρ_1, ρ_2, ρ_3, δ is a regular sequence. To show that W is an integral domain we need to show that

the localization $W[\hat{\delta}^{-1}]$ is an integral domain. Now

$$W[\hat{\delta}^{-1}] = F_q[\hat{X_2}, \hat{X_4}, \hat{X_6}, \hat{\Xi_1}, \hat{\Xi_2}, \hat{\Xi_3}, \hat{\delta}^{-1}]$$

since ρ_1, ρ_2 and ρ_3 enable us to express $\hat{Y_1}, \hat{Y_3}$ and $\hat{Y_5}$ in terms of $\hat{X_2}, \hat{X_4}, \hat{X_6}$, $\hat{\Xi_1}$, $\hat{\Xi_2}$, $\hat{\Xi_3}$ and $\hat{\delta}^{-1}$ and so eliminate $\hat{Y_1}, \hat{Y_3}$ and $\hat{Y_5}$ from the generators of the ring. Note that the images of $X_2, X_4, X_6, \Xi_1, \Xi_2$ and Ξ_3 in W are algebraically independent. Hence the sub-algebra U generated by the images of $X_2, X_4, X_6, \Xi_1, \Xi_2$ and Ξ_3 is a polynomial algebra. But $U[\hat{\delta}^{-1}] = W[\hat{\delta}^{-1}]$. Thus we see that $W[\hat{\delta}^{-1}]$ is a UFD, being a localization of a polynomial ring. In particular, W is an integral domain. Thus we deduce that ψ is an isomorphism. To prove that W is integrally closed we would like to know that $\hat{\delta}$ generates a prime ideal in W. That is, we want to prove that $T/\langle \rho_1, \rho_2, \rho_3, \delta \rangle$ is an integral domain. For this, from Equation(5.2), Equation(5.3) and Equation(5.4) we get

$$(X_2^q X_4^{q^2} - X_2^{q^2} X_4^q)\Xi_3 + \langle \rho_1, \rho_2, \rho_3, \delta \rangle$$

$$= ((X_4^{q^2} - X_2^{q^2-1} X_4)(X_2 \Xi_2^q + X_2 C_{3,0} \Xi_1 - X_2^q C_{3,1} \Xi_1 - X_2 C_{3,2} \Xi_1^q + X_2^q C_{3,2} \Xi_2) +$$

$$(X_2 X_4^q - X_2^q X_4)(-\Xi_1^{q^2} - C_{3,0}\Xi_2 + C_{3,1}\Xi_1^q + X_2^{q^2-1} C_{3,1}\Xi_1 - X_2^{q^2-1} C_{3,2}\Xi_2)) + \langle \rho_1, \rho_2, \rho_3, \delta \rangle.$$

Let $\delta' = X_2^q X_4^{q^2} - X_2^{q^2} X_4^q$. If $\rho_1, \rho_2, \rho_3, \delta, \delta'$ is a regular sequence and if the images $Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2$ in $T/\langle \rho_1, \rho_2, \rho_3, \delta, \rangle$ are algebraically independent then $T/\langle \rho_1, \rho_2, \rho_3, \delta \rangle$ is an integral domain by the argument above. But $\rho_1, \rho_2, \rho_3, \delta, \delta'$ is a not a regular sequence because X_2 and X_4 appear in both δ and δ', and the images of $Y_5, X_2, X_4, X_6, \Xi_1, \Xi_2$ in $T/\langle \rho_1, \rho_2, \rho_3, \delta \rangle$ are not algebraically independent because

$$\delta = X_2^{q^2} X_4^q X_6 - X_2^{q^2} X_4 X_6^q - X_2^q X_4^{q^2} X_6 + X_2 X_4^{q^2} X_6^q + X_2^q X_4 X_6^{q^2} - X_2 X_4^q X_6^{q^2}$$

and so

$$\hat{X}_2^{q^2} \hat{X}_4^q \hat{X}_6 - \hat{X}_2^{q^2} \hat{X}_4 \hat{X}_6^q - \hat{X}_2^q \hat{X}_4^{q^2} \hat{X}_6 + \hat{X}_2 \hat{X}_4^{q^2} \hat{X}_6^q + \hat{X}_2^q \hat{X}_4 \hat{X}_6^{q^2} - \hat{X}_2 \hat{X}_4^q \hat{X}_6^{q^2} = \langle \rho_1, \rho_2, \delta, \delta' \rangle.$$

Thus again our method fails here.

Establishing the presentation in the general case

Now we state the result, to be found in Matsumura [30], which we use to show that

$$R = F_q[y_1, y_3, \dots y_{2n-1}, x_2, x_4, \dots, x_{2n}, \xi_1, \dots \xi_{n-1}]$$

is integrally closed in the general case for all $n \geq 2$.

Lemma 5.4.6. *(Theorem 20.2 in [30]). Let R be a Noetherian integral domain, Γ a set of prime elements of R, and let S be the multiplicative set generated by Γ. If $S^{-1}R$ is a unique factorization domain then so is R.*

Theorem 5.4.7. *Let $S = F_q[x_1, \dots, x_{2n}]$ where $x_1, \dots, x_{2n}$ is the dual basis of V^* corresponding to the basis $e_1, \dots, e_{2n}$ of V. If*

$$R = F_q[y_1, y_3, \dots, y_{2n-1}, x_2, x_4, \dots, x_{2n}, \xi_1, \dots, \xi_{n-1}],$$

then R is integrally closed.

Proof. We introduce formal variables $Y_1, Y_3, \dots, Y_{2n-1}, X_2, X_4, \dots, X_{2n}, \Xi_1, \dots, \Xi_{n-1}$ and define a map

$$\phi : T = F_q[Y_1, Y_3, \dots, Y_{2n-1}, X_2, X_4, \dots, X_{2n}, \Xi_1, \dots, \Xi_{n-1}] \to R$$

by sending Y_i to y_i, X_i to x_i and Ξ_i to ξ_i. This is an epimorphism and $T/\mathrm{Ker}\phi \cong R$. Let

$$\rho_i = \Xi_i^{q^{n-i}} + \sum_{j=1}^{n} X_{2j}^{q^{n-i}} Y_{2j-1} + \sum_{j=1}^{n-i} (-1)^{j+i+1} C_{n,n-j-i} \Xi_j^{q^{n-j-i}} + \sum_{j=1}^{i-1} (-1)^j C_{n,n-j} \Xi_{i-j}^{q^{n-i}} \tag{5.5}$$

where $1 \leq i \leq n-1$. We need to show that $\mathrm{Ker}\phi = \langle \rho_1, \dots, \rho_{n-1} \rangle$. Since $\langle \rho_1, \dots, \rho_{n-1} \rangle \subseteq \mathrm{Ker}\phi$, so we have

$$W = T/\langle \rho_1, \dots, \rho_{n-1} \rangle \overset{\psi}{\twoheadrightarrow} T/\mathrm{Ker}\phi \subseteq S^N.$$

We need to prove that ψ is an isomorphism. We know that $T/\mathrm{Ker}\phi$ is an integral domain and $T/\mathrm{Ker}\phi \subseteq S$. Thus by Lemma 4.4.4 $\dim(T/\mathrm{Ker}\phi) \leq 2n$. Let

$R^{'} = F_q[y_1, \ldots, y_{2n-1}, x_2, \ldots, x_{2n}]$. Now the polynomials $P_j(X) = \underset{(V/U)}{D}(X - x_j)$ for $j = 1, 3, \ldots, 2n-1$ split over $ff(S)$, where $P_j(X) \in R^{'}[X]$, and it is easy to see that $ff(S) = ff(R^{'})(x_1, x_3, \ldots, x_{2n-1})$. Thus by definition $ff(S)$ is the splitting field for these polynomials and so by Theorem 4.3.4 the extension $ff(R^{'}) \subseteq ff(S)$ is finite and normal. Now the elements $x_1, x_3, \ldots, x_{2n-1}$ are separable. Therefore by Theorem 4.3.7 the extension $ff(R^{'}) \subseteq ff(S)$ is separable. Since the extension $ff(R^{'}) \subseteq ff(S)$ is finite and separable, so by the remark after Proposition 4.4.5 we have that $y_1, \ldots, y_{2n-1}, x_2, \ldots, x_{2n}$ are algebraically independent. Since $R^{'} \subseteq T/\mathrm{Ker}\phi$, therefore again by Lemma 4.4.4 $\dim(T/\mathrm{Ker}\phi) \geq 2n$. It follows that $\dim(T/\mathrm{Ker}\phi) = 2n$. We would like to prove that W is an integral domain of Krull dimension $2n$. Since from Equation(5.5) we have

$$\rho_i \equiv \Xi_i^{q^{n-i}} \mathrm{mod}\langle X_2, \ldots, X_{2n}\rangle$$

it follows that

$$\rho_i \equiv \Xi_i^{q^{n-i}} \mathrm{mod}\langle X_2, \ldots, X_{2n}, \Xi_1, \ldots, \Xi_{i-1}\rangle. \tag{5.6}$$

Now

$$X_2, \ldots, X_{2n}, \Xi_1, \ldots, \Xi_{n-1}$$

is a regular sequence. By Theorem 3.6.3

$$X_2, \ldots, X_{2n}, \Xi_1, \ldots, \Xi_{n-1}^{q}$$

is a regular sequence. Thus by Equation(5.6)

$$X_2, \ldots, X_{2n}, \Xi_1, \ldots, \Xi_{n-2}, \rho_{n-1}$$

is a regular sequence. Again by Theorem 3.6.3

$$X_2, \ldots, X_{2n}, \Xi_1, \ldots, \Xi_{n-2}^{q^2}, \rho_{n-1}$$

is a regular sequence. Thus again by Equation(5.6)

$$X_2, \ldots, X_{2n}, \Xi_1, \ldots, \Xi_{n-3}, \rho_{n-2}, \rho_{n-1}$$

is a regular sequence. By continuing the process we eventually get that

$$X_2, \ldots, X_{2n}, \rho_1, \ldots, \rho_{n-1}$$

is a regular sequence. So by Lemma 3.6.4 it follows that

$$\rho_1, \ldots, \rho_{n-1}, X_2, \ldots, X_{2n}$$

is a regular sequence. Thus it follows that $\rho_1, \ldots, \rho_{n-1}$ is a regular sequence. Therefore by Theorem 3.7.13 $\dim W = 2n$. Write $\hat{x}$ for the coset $x + \langle \rho_1, \ldots, \rho_{n-1} \rangle$ where $x \in T$. Then Equation(5.5) can be written in matrix form as follows:

$$\begin{bmatrix} \hat{X}_2^{q^{n-1}} & \hat{X}_4^{q^{n-1}} & \ldots & \hat{X}_{2n-2}^{q^{n-1}} \\ \hat{X}_2^{q^{n-2}} & \hat{X}_4^{q^{n-2}} & \ldots & \hat{X}_{2n-2}^{q^{n-2}} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{X}_2^{q} & \hat{X}_4^{q} & \ldots & \hat{X}_{2n-2}^{q} \end{bmatrix} \begin{bmatrix} \hat{Y}_1 \\ \hat{Y}_3 \\ \vdots \\ \hat{Y}_{2n-3} \end{bmatrix}$$

$$= \begin{bmatrix} -\hat{\Xi}_1^{q^{n-1}} - \hat{X}_{2n}^{q^{n-1}} \hat{Y}_{2n-1} - \sum_{j=1}^{n-1} (-1)^{j+2} \hat{C}_{n,n-j-1} \hat{\Xi}_j^{q^{n-j-1}} \\ -\hat{\Xi}_2^{q^{n-2}} - \hat{X}_{2n}^{q^{n-2}} \hat{Y}_{2n-1} - \sum_{j=1}^{n-2} (-1)^{j+3} \hat{C}_{n,n-j-2} \hat{\Xi}_j^{q^{n-j-2}} + \hat{C}_{n,n-1} \hat{\Xi}_1^{q^{n-2}} \\ \vdots \\ -\hat{\Xi}_{n-1}^{q} - \hat{X}_{2n}^{q} \hat{Y}_{2n-1} - (-1)^{n+1} \hat{C}_{n,0} \hat{\Xi}_1 - \sum_{j=1}^{n-2} (-1)^{j} \hat{C}_{n,n-j} \hat{\Xi}_{n-j-1}^{q} \end{bmatrix}.$$

Suppose

$$\Delta = \begin{bmatrix} X_2^{q^{n-1}} & X_4^{q^{n-1}} & \ldots & X_{2n-2}^{q^{n-1}} \\ X_2^{q^{n-2}} & X_4^{q^{n-2}} & \ldots & X_{2n-2}^{q^{n-2}} \\ \vdots & \vdots & \ddots & \vdots \\ X_2^{q} & X_4^{q} & \ldots & X_{2n-2}^{q} \end{bmatrix} \text{ and let } \delta = |\Delta|$$

Now as above

$$\rho_1, \ldots, \rho_{n-1}, X_2, \ldots, X_{2n}$$

is a regular sequences. Let $\lambda_{n-1} \neq 0$, then it follows that

$$\rho_1, \ldots, \rho_{n-1}, X_2, \ldots, X_{2n-4}, \sum_{i=1}^{n-1} \lambda_i X_{2i}$$

is a regular sequence. So by Lemma 3.6.4 it follows that

$$\rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n-1} \lambda_i X_{2i}, X_2, \ldots, X_{2n-4}$$

is a regular sequence. It follows that

$$\rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n-1} \lambda_i X_{2i}$$

is a regular sequence. Now by comparing the definition of δ with the construction of the Dickson invariants in section 2.1, we see that δ is a product of non-zero linear combinations of $X_2, \ldots, X_{2n-2}$. Thus by Lemma 3.6.6 it follows that $\rho_1, \ldots, \rho_{n-1}, \delta$ is a regular sequences. To show that W is an integral domain we need to show that the localization $W[\hat{\delta}^{-1}]$ is an integral domain. Now

$$W[\hat{\delta}^{-1}] = F_q[\hat{Y}_{2n-1}, \hat{X}_2, \hat{X}_4, \ldots, \hat{X}_{2n}, \hat{\Xi}_1, \ldots, \hat{\Xi}_{n-1}, \hat{\delta}^{-1}]$$

since the ρ_i enable us to express $\hat{Y}_1, \ldots, \hat{Y}_{2n-3}$ in terms of $\hat{X}_2, \hat{X}_4, \ldots, \hat{X}_{2n}, \hat{\Xi}_1, \ldots, \hat{\Xi}_{n-1}$ and $\hat{\delta}^{-1}$ and so eliminate $\hat{Y}_1, \ldots, \hat{Y}_{2n-3}$ from the generators of the ring. Notice that the images of $Y_{2n-1}, X_2, X_4, \ldots X_{2n}, \Xi_1, \ldots, \Xi_{n-1}$ in W are algebraically independent. Hence the sub-algebra U generated by the images of $Y_{2n-1}, X_2, X_4, \ldots X_{2n}$, $\Xi_1, \ldots, \Xi_{n-1}$ is a polynomial algebra. But $U[\hat{\delta}^{-1}] = W[\hat{\delta}^{-1}]$. Thus we see that $W[\hat{\delta}^{-1}]$ is a UFD, being a localization of a polynomial ring. In particular, W is an integral domain. By using Proposition 3.5.7 we have htKer$\psi = 0$ and so we deduce that ψ is an isomorphism. Let $\Gamma = \{\hat{X}_2, \hat{X}_4, \ldots, \hat{X}_{2n}\}$ and let $\mathcal{S}$ be the multiplicative set generated by all non-zero linear combinations of $\hat{X}_2, \hat{X}_4, \ldots, \hat{X}_{2n}$. To prove that W is integrally closed we use Lemma 5.4.6. We need to show that each non-zero linear combination $\sum_{i=1}^{n} \lambda_i \hat{X}_{2i}$ of elements of Γ is prime in W and that $\mathcal{S}^{-1}W$ is a unique factorization domain. By symmetry it is sufficient to show that $\sum_{i=1}^{n} \lambda_i \hat{X}_{2i}$ is prime when $\lambda_n \neq 0$. To see this note that if σ is any permutation of $\{1, \ldots, n\}$ then the map $e_{2i} \mapsto e_{2\sigma(i)}$, $e_{2i-1} \mapsto e_{2\sigma(i)-1}$ preserves the symplectic form and induces the map $x_{2i} \mapsto x_{2\sigma^{-1}(i)}$, $x_{2i-1} \mapsto x_{2\sigma^{-1}(i)-1}$ on V^*. Therefore given an arbitrary linear combination we can choose a permutation preserving the invariants and moving it to one in which $\lambda_n \neq 0$. To prove that $\sum_{i=1}^{n} \lambda_i \hat{X}_{2i}$ is prime in W we

need to show that $T/\langle \rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n} \lambda_i X_{2i} \rangle$ is an integral domain. Write $\bar{x}$ for the coset $x + \langle \rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n} \lambda_i X_{2i} \rangle$ where $x \in T$. Then again Equation(5.5) can be written in matrix form as follows:

$$\begin{bmatrix} \bar{X}_2^{q^{n-1}} & \bar{X}_4^{q^{n-1}} & \ldots & \bar{X}_{2n-2}^{q^{n-1}} \\ \bar{X}_2^{q^{n-2}} & \bar{X}_4^{q^{n-2}} & \ldots & \bar{X}_{2n-2}^{q^{n-2}} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{X}_2^{q} & \bar{X}_4^{q} & \ldots & \bar{X}_{2n-2}^{q} \end{bmatrix} \begin{bmatrix} \bar{Y}_1 \\ \bar{Y}_3 \\ \vdots \\ \bar{Y}_{2n-3} \end{bmatrix}$$

$$= \begin{bmatrix} -\bar{\Xi}_1^{q^{n-1}} - \bar{X}_{2n}^{q^{n-1}} \bar{Y}_{2n-1} - \sum_{j=1}^{n-1} (-1)^{j+2} \bar{C}_{n,n-j-1} \bar{\Xi}_j^{q^{n-j-1}} \\ -\bar{\Xi}_2^{q^{n-2}} - \bar{X}_{2n}^{q^{n-2}} \bar{Y}_{2n-1} - \sum_{j=1}^{n-2} (-1)^{j+3} \bar{C}_{n,n-j-2} \bar{\Xi}_j^{q^{n-j-2}} + \bar{C}_{n,n-1} \bar{\Xi}_1^{q^{n-2}} \\ \vdots \\ -\bar{\Xi}_{n-1}^{q} - \bar{X}_{2n}^{q} \bar{Y}_{2n-1} - (-1)^{n+1} \bar{C}_{n,0} \bar{\Xi}_1 - \sum_{j=1}^{n-2} (-1)^{j} \bar{C}_{n,n-j} \bar{\Xi}_{n-j-1}^{q} \end{bmatrix}.$$

Now again as above

$$\rho_1, \ldots, \rho_{n-1}, X_2, \ldots, X_{2n}$$

is a regular sequence. Thus for λ_{n-1} and $\lambda_n \neq 0$ it follows that

$$\rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n-1} \lambda_i X_{2i}, \sum_{i=1}^{n} \lambda_i X_{2i}$$

is a regular sequence. Just as in the argument to show that $\rho_1, \ldots, \rho_{n-1}, \delta$ is a regular sequence, we again use the fact that by comparing with the construction in section 2.1 we know that δ is a product of non-zero linear combinations of $X_2, \ldots, X_{2n-2}$. Thus it follows that

$$\rho_1, \ldots, \rho_{n-1}, \delta, \sum_{i=1}^{n} \lambda_i X_{2i}$$

is a regular sequence. By Lemma 3.6.4 it follows that

$$\rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n} \lambda_i X_{2i}, \delta$$

is a regular sequence. Let $W' = T/\langle \rho_1, \ldots, \rho_{n-1}, \sum_{i=1}^{n} \lambda_i X_{2i} \rangle$. To show that W' is an integral domain it is sufficient to show that the localization $W'[\bar{\delta}^{-1}]$ is an integral domain. Now since the ρ_i enable us to express $\bar{Y}_1, \ldots, \bar{Y}_{2n-3}$ in terms of $\bar{X}_2, \bar{X}_4, \ldots, \bar{X}_{2n-2}$, $\bar{\Xi}_1, \ldots, \bar{\Xi}_{n-1}$ and $\bar{\delta}^{-1}$ so we get

$$W'[\bar{\delta}^{-1}] = F_q[\bar{X}_2, \bar{X}_4, \ldots, \bar{X}_{2n-2}, \bar{\Xi}_1, \ldots, \bar{\Xi}_{n-1}, \bar{Y}_{2n-1}, \bar{\delta}^{-1}]$$

Note that the images of $X_2, X_4, \ldots X_{2n-2}, \Xi_1, \ldots, \Xi_{n-1}, Y_{2n-1}$ in $W^{'}$ are algebraically independent. Hence the sub-algebra $U^{'}$ generated by the images of $X_2, X_4, \ldots X_{2n-2}$, $\Xi_1, \ldots, \Xi_{n-1}, Y_{2n-1}$ is a polynomial algebra. It is clear that $U^{'}[\bar{\delta}^{-1}] = W^{'}[\bar{\delta}^{-1}]$, hence we see that $W^{'}[\bar{\delta}^{-1}]$ is a UFD, being a localization of a polynomial ring. In particular, $W^{'}$ is an integral domain. Now

$$\mathcal{S}^{-1}W = \mathcal{S}^{-1}F_q[\hat{X}_2, \hat{X}_4, \ldots, \hat{X}_{2n}, \hat{\Xi}_1, \ldots, \hat{\Xi}_{n-1}, \hat{Y}_{2n-1}]$$

since $\hat{\delta} \in \mathcal{S}$ and so the ρ_i enable us to express $\hat{Y}_1, \ldots, \hat{Y}_{2n-3}$ in terms of $\hat{X}_2, \hat{X}_4, \ldots, \hat{X}_{2n}$, $\hat{\Xi}_1, \ldots, \hat{\Xi}_{n-1}$ and $\hat{\delta}^{-1}$. It should be noted the images of $X_2, X_4, \ldots X_{2n}, \Xi_1, \ldots, \Xi_{n-1}$, Y_{2n-1} in W are algebraically independent. Hence the sub-algebra U generated by the images of $X_2, X_4, \ldots X_{2n}$, $\Xi_1, \ldots, \Xi_{n-1}, Y_{2n-1}$ is a polynomial algebra. It is easy to see that $\mathcal{S}^{-1}U = \mathcal{S}^{-1}W$, hence $\mathcal{S}^{-1}W$ is a UFD, being a localization of a polynomial ring. □

Theorem 5.4.8. *Let $S = F_q[x_1, \ldots, x_{2n}]$ where $x_1, \ldots, x_{2n}$ is the dual basis of V^* corresponding to the basis $e_1, \ldots, e_{2n}$ of V. Then*

$$S^N = F_q[y_1, y_3, \ldots y_{2n-1}, x_2, x_4, \ldots, x_{2n}, \xi_1, \ldots \xi_{n-1}].$$

Proof. Follows from Lemma 5.4.1, Theorem 5.4.2, Theorem 5.4.7 and Lemma 4.2.2. □

Remark 5.4.9. It can be easily seen from the above theorem and Lemma 5.3.1 that S^N is a graded complete intersection, and so in particular it is Gorenstein and Cohen-Macaulay.

Remark 5.4.10. We still do not know about S^G in our second case. Thus this problem is still open.

Chapter 6

Invariant rings of orthogonal groups over F_{2^l}

Let V be a vector space over the field F_2. We know S^G where $S = F_2[V]$ and G is the orthogonal group preserving a non-singular quadratic form on V. It was computed by Kropholler, Mohseni Rajaei and Segal in [24]. In this chapter we generalize some of their results which will help us to compute S^G over any finite field of characteristic 2.

6.1 The Steenrod algebra and Chern polynomials

Let V be a vector space over the field F_{2^l} and $S = F_{2^l}[V]$.

Definition 6.1.1. The *Steenrod algebra* is an F_{2^l}-algebra generated by elements $\mathcal{P}^i$, for $i \geq 0$ where $\mathcal{P}^i$ is homogeneous of degree $(2^l - 1)i$. The action on S is determined by the following facts.

(i) $\mathcal{P}^0$ acts as the identity operation on S.

(ii) Each $\mathcal{P}^i$ is a linear transformation.

(iii) For all $x \in V^*$, $\mathcal{P}^1(x) = x^{2^l}$ and $\mathcal{P}^n(x) = 0$ for $n \geq 2$.

(iv) The Cartan formula holds: for all s and t in S,

$$\mathcal{P}^n(st) = \sum_{i=0}^{n} (\mathcal{P}^i s)(\mathcal{P}^{n-i} t).$$

(v) For any homogeneous element s of S of degree d, $\mathcal{P}^d(s) = s^{2^l}$ and $\mathcal{P}^j(s) = 0$ if $j > d$.

(vi) The total Steenrod operation $\mathcal{P}^\bullet = \mathcal{P}^0 + \mathcal{P}^1 + \mathcal{P}^2 + \dots$ acts as a ring endomorphism of S.

Definition 6.1.2. Suppose that $\mathcal{S}$ is a non-empty subset of V^* which contains d elements. The *Chern polynomial* associated to $\mathcal{S}$ is the polynomial

$$\prod_{x \in \mathcal{S},\ \lambda \in F_{2^l}^*} (X + \lambda x).$$

Let's write f_i for the coefficient of $X^{(2^l-1)d-i}$ so that

$$\prod_{x \in \mathcal{S},\ \lambda \in F_{2^l}^*} (X + \lambda x) = f_0 X^{(2^l-1)d} + f_1 X^{(2^l-1)d-1} + \dots + f_{(2^l-1)d}.$$

Let's write $f_\infty = \prod_{x \in \mathcal{S}} x$. Then $f_\infty^{2^l-1} = f_{(2^l-1)d}$.

Lemma 6.1.3. *For each i in the range $0 \le i \le d$,*

$$\mathcal{P}^i(f_\infty) = f_\infty f_{(2^l-1)i}.$$

Proof. Since $\mathcal{P}^\bullet$ is a ring homomorphism, by applying the total Steenrod operation to f_∞ we get

$$\begin{aligned}
\mathcal{P}^\bullet(f_\infty) &= \prod_{x \in \mathcal{S}} (x + x^{2^l}) \\
&= f_\infty \cdot \prod_{x \in \mathcal{S}} (1 + x^{2^l-1}) \\
&= f_\infty \cdot \prod_{x \in \mathcal{S},\ \lambda \in F_{2^l}^*} (1 + \lambda x) \\
&= f_\infty \cdot (f_0 + f_1 + \dots + f_{(2^l-1)d}).
\end{aligned}$$

This completes the proof. □

6.2 Rank of a bilinear form

Definition 6.2.1. The *rank* of a bilinear form B is the rank of the matrix which represents that form.

Lemma 6.2.2. *The rank of an alternating matrix with entries in a field is even.*

Proof. Follows from Corollary 1 of Theorem 6.3 in [21]. □

Note that alternating forms are determined up to equivalence by rank and according to the above lemma, the rank is even.

Lemma 6.2.3. *Let Q and $Q^{'}$ be quadratic forms on a vector space V over F_{2^l}. Then the following are equivalent:*

(i) Q and $Q^{'}$ have the same polarization;

(ii) $Q + Q^{'} = x^2$ for some $x \in V^*$.

Proof. (i) $\implies$ (ii) Let B and $B^{'}$ be the polarizations of Q and $Q^{'}$ respectively. Since

$$(B + B^{'})(u, v) = B(u, v) + B^{'}(u, v).$$

It is sufficient to prove that if $(B + B^{'})(u, v) = 0$, then $Q + Q^{'} = x^2$. Let

$$Q + Q^{'} = \sum_i \sum_j b_{ij} x_i x_j.$$

Then

$$\begin{aligned}
(B + B^{'})(e_k, e_l) &= \sum_i \sum_j b_{ij} x_i x_j (e_k + e_l) + \sum_i \sum_j b_{ij} x_i x_j (e_k) + \sum_i \sum_j b_{ij} x_i x_j (e_l) \\
&= \sum_i \sum_j b_{ij} x_i (e_k + e_l) x_j (e_k + e_l) + \sum_i \sum_j b_{ij} x_i (e_k) x_j (e_k) + \sum_i \sum_j b_{ij} x_i (e_l) x_j (e_l) \\
&= \sum_i \sum_j b_{ij} (\delta_{ik}\delta_{jk} + \delta_{il}\delta_{jk} + \delta_{ik}\delta_{jl} + \delta_{il}\delta_{jl}) + \sum_i \sum_j b_{ij} \delta_{ik}\delta_{jk} + \sum_i \sum_j b_{ij} \delta_{il}\delta_{jl} \\
&= \sum_i \sum_j b_{ij} \delta_{il}\delta_{jk} + \sum_i \sum_j b_{ij} \delta_{ik}\delta_{jl}
\end{aligned}$$

$$= \sum_j b_{lj}\delta_{ll}\delta_{jk} + \sum_j b_{kj}\delta_{kk}\delta_{jl}$$

$$= b_{lk} + b_{kl}.$$

Therefore

$$(B + B^{'})(e_k, e_l) = 0 \implies b_{lk} = b_{kl} \text{ for } l \neq k.$$

Thus

$$Q + Q^{'} = \sum_i b_{ii}x_i^2.$$

By using Lemma 1.2.9 (i) each element of F_{2^l} is a square, so there exist $a_{ii} \in F_{2^l}$ such that $b_{ii} = a_{ii}^2$. Therefore

$$Q + Q^{'} = \sum_i a_{ii}^2 x_i^2.$$

Now using Lemma 1.3.9, we get

$$Q + Q^{'} = (\sum_i a_{ii}x_i)^2.$$

So

$$Q + Q^{'} = x^2 \text{ for some } x \in V^*.$$

(ii) $\implies$ (i) Let $Q + Q^{'} = x^2$ for some $x \in V^*$, then it is sufficient to prove that $(B + B^{'})(u, v) = 0$. Since

$$(B + B^{'})(u, v) = (Q + Q^{'})(u + v) + (Q + Q^{'})(u) + (Q + Q^{'})(v)$$

$$= x^2(u + v) + x^2(u) + x^2(v)$$
$$= x(u + v)x(u + v) + x(u)x(u) + x(v)x(v)$$
$$= 0. \qquad \square$$

We consider quadratic forms in the presence of a fixed alternating form to which it polarizes. We shall use the term symplectic space to refer to a finite dimensional vector space endowed with an alternating form of maximum possible rank. The group of automorphisms of a symplectic space is called a symplectic group. On a symplectic space, we say that two quadratic forms Q and $Q^{'}$ are equivalent if and

only if there exists some g in the symplectic group such that $Q^{'}(v) = Q(gv)$ for all v. It follows from Theorem 1.4.14 (ii) that on a non-zero even dimension symplectic space there are two types of non-singular quadratic forms up to equivalence, called +type and −type.

Theorem 6.2.4. *Let V be a vector space of dimension $2n$ over the field F_{2^l}. Given a non-degenerate alternating form B on V, there are $(2^l)^{2n}$ quadratic forms which polarize to B, and of these quadratic forms $2^{2ln-1} + 2^{ln-1}$ are of +type and $2^{2ln-1} - 2^{ln-1}$ are of −type.*

Proof. It follows from the above lemma that there are $(2^l)^{2n}$ quadratic forms which polarize to B. Now let $G = S_P(2n, F_{2^l})$ and $\Gamma = \{Q : Q$ is a quadratic form polarizing to $B\}$. Then G acts on Γ as $Q^g(v) = Q(gv)$ for $g \in G$ and $v \in V$. Thus we get two orbits, say $\mathrm{Orb}(Q^+)$ and $\mathrm{Orb}(Q^-)$, where

$$\begin{aligned} \mathrm{Orb}(Q^+) &= \{P^+ \in \Gamma : P^+ \sim Q^+\} \\ &= \{P^+ \in \Gamma : (P^+)^g = Q^+ \text{ for some } g \in G\} \end{aligned}$$

and

$$\begin{aligned} \mathrm{Orb}(Q^-) &= \{P^- \in \Gamma : P^- \sim Q^-\} \\ &= \{P^- \in \Gamma : (P^-)^g = Q^- \text{ for some } g \in G\}. \end{aligned}$$

Now let

$$G_{Q^+} = \{g \in G : (Q^+)^g = Q^+\}$$

and

$$G_{Q^-} = \{g \in G : (Q^-)^g = Q^-\}.$$

Then by Theorem 1.4.5, we have

$$|\mathrm{Orb}(Q^+)| = |G : G_{Q^+}|$$

and

$$|\mathrm{Orb}(Q^-)| = |G : G_{Q^-}|.$$

Thus the number of quadratic forms of +type is $|G : G_{Q^+}| = |G : O^+|$.

Hence by using Theorem 1.5.5 and Theorem 1.5.10, we see that the number of quadratic forms of +type is

$$\frac{(2^l)^{n^2}\prod_{i=1}^{n}((2^l)^{2i}-1)}{2(2^l)^{n(n-1)}((2^l)^n-1)\prod_{i=1}^{n-1}((2^l)^{2i}-1)}$$
$$= 2^{2ln-1}+2^{ln-1}.$$

Now the number of quadratic forms of $-$type is $|G:G_{Q^-}| = |G:O^-|$.

Hence by using Theorem 1.5.5 and Theorem 1.5.10, we see that the number of quadratic forms of $-$type is

$$\frac{(2^l)^{n^2}\prod_{i=1}^{n}((2^l)^{2i}-1)}{2(2^l)^{n(n-1)}((2^l)^n+1)\prod_{i=1}^{n-1}((2^l)^{2i}-1)}$$
$$= 2^{2ln-1}-2^{ln-1}.$$

□

6.3 Orthogonal and symplectic groups

In this section we state our definitions of symplectic and orthogonal groups and consider some of their representations.

Let n be a positive integer. Henceforth we suppose that V has dimension $2n+1$ over F_{2^l} and that ξ_0 is a non-singular quadratic form on V. Let B denote the polarization of ξ_0. The radical of B is one dimensional. Choose a basis $e_0,\ldots,e_{2n}$ of V where e_0 is the non-zero vector in Rad$B$.

We refer the reader to Cameron's notes [6] for the background of the following lemma and definition.

Lemma 6.3.1. *It is possible to choose the e_i for $i \geq 1$ so that the matrix M with (i,j)-entry $b_{i,j} = B(e_i,e_j)$ is*

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

filled out with zeros.

We write M_0 for the non-singular alternating matrix obtained by omitting the first row and column of M.

Definition 6.3.2. (i) $O(V, \xi_0)$ denotes the orthogonal group of automorphisms of V which preserves the quadratic form ξ_0.

(ii) $S_P(V, B)$ denotes the symplectic group of automorphisms of V which preserves the alternating form B.

(iii) U denotes the quotient space $V/\langle e_0 \rangle$. This space inherits the alternating form, but it does not inherit any natural quadratic form.

(iv) $S_P(U, \bar{B})$ denotes the symplectic group of automorphisms of U which preserves the inherited alternating form $\bar{B}$.

Let $x_0, \ldots, x_{2n}$ be the basis of V^* which is dual to our chosen basis of V. Suppose $S = F_{2^l}[x_0, \ldots, x_{2n}]$. We remark that when the basis e_i is chosen in accordance with Lemma 6.3.1, then the quadratic form is given by

$$\xi_0 = x_0^2 + x_1 x_2 + x_3 x_4 + \cdots + x_{2n-1} x_{2n}.$$

The canonical surjection $V \to U$ induces an injection $U^* \to V^*$. We identify U^* with its image in V^*: thus U^* is the subspace of V^* spanned by $x_1, \ldots, x_{2n}$. The symmetric algebra on U^* is the subring of S generated by $x_1, \ldots, x_{2n}$. Let $T = F_{2^l}[x_1, \ldots, x_{2n}]$.

Now If V is an odd-dimensional symplectic space, then according to Theorem 1.4.14 (i) there is only one kind of non-singular quadratic form up to equivalence. If ξ_0 is such a form and B is its polarization, then according to Lemma 6.2.3, each form having the same polarization is equal to $\xi_0 + x^2$ for some $x \in V^*$. There are three kinds of quadratic forms: the non-singular forms (all equivalent to ξ_0), the singular forms of +type, and the singular forms of −type.

Lemma 6.3.3. *If* $\dim V = 2n + 1 \geq 3$ *then*

(i) $2^{2ln-1} + 2^{ln-1}$ *of these forms have +type, and each is equal to* $\xi_0 + x_0^2 + x^2$ *for some* $x \in U^*$*;*

(ii) $2^{2ln-1} - 2^{ln-1}$ *of these forms have −type, and each is equal to* $\xi_0 + x_0^2 + x^2$ *for some* $x \in U^*$*;*

(iii) $2^{2ln+l} - 2^{2ln}$ *of these forms are non-singular, and each is equal to* $\xi_0 + x^2$ *for some* $x \in V^*$ *such that* $x \neq x_0 + y$ *for any* $y \in U^*$*.*

Proof. (i) Suppose

$$\xi_0 = x_0^2 + x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}$$

is a non-singular quadratic form on V. Now let

$$\xi = x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}$$

be a singular quadratic form on V which is non-singular of +type on U. Thus according to Lemma 6.2.3 if B is its polarization then each form having the same polarization must be of the form $\xi + x^2$ for some $x \in U^*$. Now ξ is of +type, so according to Theorem 6.2.4 the number of such forms is $2^{2ln-1}+2^{ln-1}$. Therefore $2^{2ln-1} + 2^{ln-1}$ of these forms have +type, and each is equal to $\xi + x^2$ for some $x \in U^*$. But $\xi = \xi_0 + x_0^2$. Therefore each of these forms is equal to $\xi_0 + x_0^2 + x^2$ for some $x \in U^*$.

(ii) Suppose

$$\xi = x_1x_2 + x_3x_4 + \cdots + x_{2n-3}x_{2n-2} + x_{2n-1}^2 + x_{2n-1}x_{2n} + \beta x_{2n}^2$$

where $x_{2n-1}^2 + x_{2n-1} + \beta$ is irreducible in $F_{2^l}[x_{2n-1}]$. Here ξ is a singular quadratic form on V but is non-singular on U of $-$type. Thus according to Lemma 6.2.3 each form having the same polarization must be of the form $\xi + x^2$ for some $x \in U^*$. Now ξ is of $-$type, so according to Theorem 6.2.4 the number of such forms is $2^{2ln-1} - 2^{ln-1}$. Therefore $2^{2ln-1} - 2^{ln-1}$ of these forms have $-$type, and each is equal to $\xi + x^2$ for some $x \in U^*$. But $\xi = \xi_0 + x_0^2 + x_{2n-1}^2 + \beta x_{2n}^2$. Thus each of these forms is equal to $\xi_0 + x_0^2 + x_{2n-1}^2 + \beta x_{2n}^2 + x^2$ for some $x \in U^*$. Now according to Lemma 1.2.9 (i) each element in F_{2^l} is a square. So there exists $\beta' \in F_{2^l}$ such that $\beta'^2 = \beta$. Thus each form is equal to $\xi_0 + (x_0 + x_{2n-1} + \beta' x_{2n} + x)^2$ for some $x \in U^*$. Writing $x' = x_{2n-1} + \beta' x_{2n} + x$, then obviously $x' \in U^*$, so we see each form is equal to $\xi_0 + (x_0 + x')^2$ for some $x' \in U^*$. This completes the proof.

(iii) From (i) and (ii) the number of quadratic forms of $+$type and $-$type having the same polarization is equal to 2^{2ln}, but the total number of such forms is 2^{2ln+l}. Thus the number of quadratic forms which are non-singular on V is $2^{2ln+l} - 2^{2ln}$. Now since ξ_0 is a non-singular quadratic form on V then, again according to Lemma 6.2.3, each form having the same polarization is equal to $\xi_0 + x^2$ for some $x \in V^*$. But the fact that $x = x_0 + y$ for any $y \in U^*$ makes the form singular. Thus $2^{2ln+l} - 2^{2ln}$ of these forms are non-singular and each is equal to $\xi_0 + x^2$ for some $x \in V^*$ such that $x \neq x_0 + y$ for any $y \in U^*$

□

Definition 6.3.4. The sequence $\xi_1, \xi_2, \xi_3, \ldots$ is defined recursively by

$$\xi_n = \mathcal{P}^{(2^l)^{n-1}}(\xi_{n-1}).$$

When the basis e_i is chosen in accordance with Lemma 6.3.1, then

$$\xi_j = x_1^{(2^l)^j}x_2 + x_1x_2^{(2^l)^j} + x_3^{(2^l)^j}x_4 + x_3x_4^{(2^l)^j} + \cdots + x_{2n-1}^{(2^l)^j}x_{2n} + x_{2n-1}x_{2n}^{(2^l)^j}$$

for each $j \geq 1$. In general, for $j \geq 1$, each ξ_j belongs to the symmetric algebra on U^*. For each $j \geq 1$, ξ_j has degree $(2^l)^j + 1$.

Now

$$\prod_{x \in U^*} (X + x) = X \cdot \prod_{x \in \mathcal{S},\ \lambda \in F_{2^l}^*} (X + \lambda x)$$

where $\mathcal{S}$ is a set consisting of one non-zero vector of U^* from each 1-dimensional subspace of U^*. But the number of k-dimensional subspaces of a vector space W over a finite field F_q can be found by the following formula:

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})},$$

where n is the dimension of the vector space W. Therefore

$$| \mathcal{S} | = \frac{2^{2ln} - 1}{2^l - 1}.$$

Thus

$$\prod_{x \in U^*} (X + x) = f_0 X^{2^{2ln}} + f_1 X^{2^{2ln} - 1} + \dots + f_{(2^{2ln} - 1)} X.$$

Let $f_\infty = \prod_{x \in \mathcal{S}} x$. Then $f_\infty^{2^l - 1} = f_{(2^{2ln} - 1)}$ and we have the following lemma.

Lemma 6.3.5. *Let $U = V/\langle e_0 \rangle$ as defined in Definition 6.3.2. For $0 \leq i \leq 2n$*

$$\mathcal{P}^{\frac{(2^l)^{2n} - (2^l)^i}{2^l - 1}}(f_\infty) = f_\infty c_{U,i}.$$

Proof. By Lemma 6.1.3, for each i in the range $0 \leq i \leq | \mathcal{S} |$ we have

$$\mathcal{P}^i(f_\infty) = f_\infty f_{(2^l - 1)i}.$$

But by Lemma 2.1.2, we have

$$\prod_{x \in U^*} (X + x) = \sum_{j=0}^{2n} c_{U,j} X^{(2^l)^j}.$$

This means that

$$c_{U,0} = f_{(2^{2ln} - 1)},\ c_{U,1} = f_{(2^{2ln} - 2^l)},\ c_{U,2} = f_{(2^{2ln} - 2^{2l})}, \dots, c_{U,2n} = f_0$$

and the rest of f_i's are zero. Thus for each $0 \leq i \leq 2n$, we have

$$\mathcal{P}^{\frac{(2^l)^{2n} - (2^l)^i}{2^l - 1}}(f_\infty) = f_\infty c_{U,i}.$$

□

In the above lemma the $c_{U,i}$'s are Dickson invariants as we defined in the proof of Lemma 2.1.2. Clearly $c_{U,0} = f_\infty^{2^l-1}$. Let N_0 denote the matrix

$$\begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_{2n} \\ x_1^{2^l} & x_2^{2^l} & x_3^{2^l} & \cdots & x_{2n}^{2^l} \\ x_1^{(2^l)^2} & x_2^{(2^l)^2} & x_3^{(2^l)^2} & \cdots & x_{2n}^{(2^l)^2} \\ x_1^{(2^l)^3} & x_2^{(2^l)^3} & x_3^{(2^l)^3} & \cdots & x_{2n}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{(2^l)^{2n-1}} & x_2^{(2^l)^{2n-1}} & x_3^{(2^l)^{2n-1}} & \cdots & x_{2n}^{(2^l)^{2n-1}} \end{bmatrix},$$

then f_∞ is a scalar multiple of $\det N_0$ and by appropriate scaling of one of the vectors in $\mathcal{S}$ we may assume that $\det N_0 = f_\infty$. Thus $f_\infty \cdot \prod_{x \in U^*} (X + x)$ is equal to the determinant

$$\begin{vmatrix} X & x_1 & x_2 & x_3 & \cdots & x_{2n} \\ X^{2^l} & x_1^{2^l} & x_2^{2^l} & x_3^{2^l} & \cdots & x_{2n}^{2^l} \\ X^{(2^l)^2} & x_1^{(2^l)^2} & x_2^{(2^l)^2} & x_3^{(2^l)^2} & \cdots & x_{2n}^{(2^l)^2} \\ X^{(2^l)^3} & x_1^{(2^l)^3} & x_2^{(2^l)^3} & x_3^{(2^l)^3} & \cdots & x_{2n}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ X^{(2^l)^{2n}} & x_1^{(2^l)^{2n}} & x_2^{(2^l)^{2n}} & x_3^{(2^l)^{2n}} & \cdots & x_{2n}^{(2^l)^{2n}} \end{vmatrix}.$$

Lemma 6.3.6. *The following matrix identity holds.*

$$N_0^T \begin{bmatrix} c_{U,0} \\ c_{U,1} \\ c_{U,2} \\ \vdots \\ c_{U,2n-1} \end{bmatrix} = \begin{bmatrix} x_1^{(2^l)^{2n}} \\ x_2^{(2^l)^{2n}} \\ x_3^{(2^l)^{2n}} \\ \vdots \\ x_{2n}^{(2^l)^{2n}} \end{bmatrix}.$$

Proof. Clear. □

For later use, we write N for the $(2n+1) \times 2n$-matrix

$$\begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_{2n} \\ x_1^{2^l} & x_2^{2^l} & x_3^{2^l} & \cdots & x_{2n}^{2^l} \\ x_1^{(2^l)^2} & x_2^{(2^l)^2} & x_3^{(2^l)^2} & \cdots & x_{2n}^{(2^l)^2} \\ x_1^{(2^l)^3} & x_2^{(2^l)^3} & x_3^{(2^l)^3} & \cdots & x_{2n}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{(2^l)^{2n-1}} & x_2^{(2^l)^{2n-1}} & x_3^{(2^l)^{2n-1}} & \cdots & x_{2n}^{(2^l)^{2n-1}} \\ x_1^{(2^l)^{2n}} & x_2^{(2^l)^{2n}} & x_3^{(2^l)^{2n}} & \cdots & x_{2n}^{(2^l)^{2n}} \end{bmatrix}$$

and we write $\widehat{N}$ for the $(2n+1) \times (2n+1)$-matrix

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 & \cdots & x_{2n} \\ x_0^{2l} & x_1^{2^l} & x_2^{2^l} & x_3^{2^l} & \cdots & x_{2n}^{2^l} \\ x_0^{(2^l)^2} & x_1^{(2^l)^2} & x_2^{(2^l)^2} & x_3^{(2^l)^2} & \cdots & x_{2n}^{(2^l)^2} \\ x_0^{(2^l)^3} & x_1^{(2^l)^3} & x_2^{(2^l)^3} & x_3^{(2^l)^3} & \cdots & x_{2n}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_0^{(2^l)^{2n}} & x_1^{(2^l)^{2n}} & x_2^{(2^l)^{2n}} & x_3^{(2^l)^{2n}} & \cdots & x_{2n}^{(2^l)^{2n}} \end{bmatrix}.$$

6.4 Some families of polynomials arising from determinants

Let m be a positive integer. In the abstract commutative polynomial ring

$$\mathbb{Z}[X, \xi_1, \xi_2, \xi_3, \dots],$$

consider the polynomial

$$H_m = \begin{vmatrix} 2X & \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_m \\ \xi_1 & 2X^{2^l} & \xi_1^{2^l} & \xi_2^{2^l} & \cdots & \xi_{m-1}^{2^l} \\ \xi_2 & \xi_1^{2^l} & 2X^{(2^l)^2} & \xi_1^{(2^l)^2} & \cdots & \xi_{m-2}^{(2^l)^2} \\ \xi_3 & \xi_2^{2^l} & \xi_1^{(2^l)^2} & 2X^{(2^l)^3} & \cdots & \xi_{m-3}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_m & \xi_{m-1}^{2^l} & \xi_{m-2}^{(2^l)^2} & \xi_{m-3}^{(2^l)^3} & \cdots & 2X^{(2^l)^m} \end{vmatrix}.$$

This is the determinant of a symmetric matrix. On passing to the ring

$$F_{2^l}[X, \xi_1, \xi_2, \xi_3, \ldots.]$$

the matrix is alternating. Since, according to Lemma 6.2.2, alternating matrices have even rank, it follows that the determinant is zero modulo 2 whenever m is even, and we can make the following definition:

Definition 6.4.1. For each even integer $m \geq 0$, we write $\Omega_m(X)$ for the image of the polynomial $\frac{1}{2}H_m$ in $F_{2^l}[X, \xi_1, \xi_2, \xi_3, \ldots]$. As an example, in case $m = 2$ we find that

$$\Omega_2(X) = \xi_1^2 X^{(2^l)^2} + \xi_2^2 X^{2^l} + \xi_1^{(2^{l+1})} X + \xi_1^{(2^l+1)} \xi_2.$$

When m is odd, the image of H_m in $F_{2^l}[X, \xi_1, \xi_2, \xi_3, \ldots]$ is non-zero and does not involve X. In fact it is the square of a polynomial in $F_{2^l}[X, \xi_1, \xi_2, \xi_3, \ldots]$.

Lemma 6.4.2. *The determinant of an alternating matrix with entries in a field is a square. We call the square root of this determinant the pfaffian.*

Proof. Follows from corollary 1 of Theorem 6.3 in [21]. □

Thus we can make the following definition:

Definition 6.4.3. For each even integer m, we write Λ_m for the square root of the image of the polynomial H_{m-1} in $F_{2^l}[X, \xi_1, \xi_2, \xi_3, \ldots]$, that is, the pfaffian of the matrix defining Λ_m. For example, $\Lambda_2 = \xi_1$, $\Lambda_4 = \xi_1^{(2^l)^2+1} + \xi_2^{2^l+1} + \xi_1^{2^l}\xi_3$ etc.

6.5 How to understand Λ_m

Working in S, recall from section 6.3 that the matrix N_0 has determinant equal to f_∞. As before let M_0 denote the $2n \times 2n$ matrix with (i, j)-entry $B(e_i, e_j)$, $i, j \geq 1$. Then M_0 is a non-singular alternating matrix and so it has determinant 1. Moreover

$$N_0M_0N_0^T = \begin{bmatrix} 0 & \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_{2n-1} \\ \xi_1 & 0 & \xi_1^{2^l} & \xi_2^{2^l} & \cdots & \xi_{2n-2}^{2^l} \\ \xi_2 & \xi_1^{2^l} & 0 & \xi_1^{(2^l)^2} & \cdots & \xi_{2n-3}^{(2^l)^2} \\ \xi_3 & \xi_2^{2^l} & \xi_1^{(2^l)^2} & 0 & \cdots & \xi_{2n-4}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{2n-1} & \xi_{2n-2}^{2^l} & \xi_{2n-3}^{(2^l)^2} & \xi_{2n-4}^{(2^l)^3} & \cdots & 0 \end{bmatrix}$$

and so

$$\det(N_0M_0N_0^T) = f_\infty^2.$$

As $N_0M_0N_0^T$ is clearly congruent to the matrix of H_{2n-1} modulo 2, it follows that $\Lambda_{2n} = f_\infty$ in S and f_∞ itself can be expressed as a polynomial in the $S_P(U, \overline{B})$-invariants $\xi_1, \ldots, \xi_{2n-1}$. Playing this game with N in place of N_0, we have

$$NM_0N^T = \begin{bmatrix} 0 & \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_{2n-1} & \xi_{2n} \\ \xi_1 & 0 & \xi_1^{2^l} & \xi_2^{2^l} & \cdots & \xi_{2n-2}^{2^l} & \xi_{2n-1}^{2^l} \\ \xi_2 & \xi_1^{2^l} & 0 & \xi_1^{(2^l)^2} & \cdots & \xi_{2n-3}^{(2^l)^2} & \xi_{2n-2}^{(2^l)^2} \\ \xi_3 & \xi_2^{2^l} & \xi_1^{(2^l)^2} & 0 & \cdots & \xi_{2n-4}^{(2^l)^3} & \xi_{2n-3}^{(2^l)^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \xi_{2n-1} & \xi_{2n-2}^{2^l} & \xi_{2n-3}^{(2^l)^2} & \xi_{2n-4}^{(2^l)^3} & \cdots & 0 & \xi_1^{(2^l)^{2n-1}} \\ \xi_{2n} & \xi_{2n-1}^{2^l} & \xi_{2n-2}^{(2^l)^2} & \xi_{2n-3}^{(2^l)^3} & \cdots & \xi_1^{(2^l)^{2n-1}} & 0 \end{bmatrix}.$$

Definition 6.5.1. We define polynomials $\Lambda_{2n,i}$ for each $n \geq 2$ and $0 \leq i \leq 2n$ by

$$\Lambda_{2n,i} = \mathcal{P}^{\frac{(2^l)^{2n} - (2^l)^i}{2^l - 1}}(\Lambda_{2n}).$$

Lemma 6.5.2. *Let $U = V/\langle e_0 \rangle$ as defined in Definition 6.3.2 For each i in the range $0 \leq i \leq 2n$, we have $\Lambda_{2n,i} = f_\infty c_{U,i}$. Each $\Lambda_{2n,i}$ can also be interpreted as the pfaffian coming from the appropriate $2n \times 2n$ matrix obtained by omitting a row and the corresponding column from NM_0N^T.*

Proof. We noted above that $\Lambda_{2n} = f_\infty$. By Lemma 6.3.5 it follows that $\Lambda_{2n,i} = f_\infty c_{U,i}$. The second statement is clear. □

6.6 The Chern Polynomials

In this section we define Chern polynomials whose coefficients can be plainly seen to be invariants of the orthogonal group $O(V, \xi_0)$ and quadratic Chern polynomials whose coefficients are plainly invariants of the symplectic group $S_P(U, \bar{B})$.

Definition 6.6.1. Let A^+ denote the set

$$\{x \in V^* : \xi_0 + x^2 \text{ has} + \text{type}\}$$

and let A^- denote the set

$$\{x \in V^* : \xi_0 + x^2 \text{ has} - \text{type}\}.$$

Let $A = A^+ \cup A^-$. Polynomials $P^+(t)$ and $P^-(t)$ in the polynomial ring $S[t]$ in one variable t of degree 1 are defined as follows:

$$P^+(t) := \prod_{x \in A^+} (t + x), \qquad P^-(t) := \prod_{x \in A^-} (t + x),$$

$$P(t) := \prod_{x \in A} (t + x).$$

The orthogonal group $O(V, \xi_0)$ permutes the elements of A^+ and A^-, so it is clear that the coefficients of $P^+(t)$ and $P^-(t)$ belong to the invariant ring $S^{O(V,\, \xi_0)}$. Note that $P(t) = P^+(t)P^-(t)$.

Definition 6.6.2. Let C^+ be the set of all quadratic forms on V of $+$type and C^- the set of all those of $-$type. Let $C = C^+ \cup C^-$. From Lemma 6.3.3 we note that $C = \{\xi_0 + x_0^2 + x^2 : x \in U^*\}$. We define quadratic Chern polynomials $Q^+(X)$, $Q^-(X)$ and $Q(X)$ in the polynomial ring $T[X]$ in one variable X of degree 2 as follows:

$$Q^+(X) := \prod_{q \in C^+} (X + q), \qquad Q^-(X) := \prod_{q \in C^-} (X + q),$$

$$Q(X) := \prod_{q \in C} (X + q).$$

The symplectic group $S_P(U, \bar{B})$ permutes the elements of C^+ and C^-. Thus the coefficients of $Q^+(X)$ and $Q^-(X)$ are invariants of the symplectic group $S_P(U, \bar{B})$. Note also that $Q(X) = Q^+(X)Q^-(X)$.

Lemma 6.6.3. *(i) The coefficients of $Q^-(X)$ belong to the subring of $F_{2^l}[x_1, \ldots, x_{2n}]$ generated by*

$$\xi_1, \ldots, \xi_{2n-1}, c_{U,2n-1}, \ldots, c_{U,n}.$$

Moreover they are linear in the Dickson invariants $c_{U,2n-1}, \ldots, c_{U,n}$.

(ii) The polynomial $f_\infty Q^-(X)$ has all coefficients in the ring $F_{2^l}[\xi_1, \ldots, \xi_{2n}]$.

(iii) The coefficients of $Q^+(X)$ belong to the subring of $F_{2^l}[x_1, \ldots, x_{2n}]$, where $l \geq 2$, generated by

$$\xi_1, \ldots, \xi_{2n-1}, c_{U,2n-1}, \ldots, c_{U,n}.$$

Moreover they are linear in the Dickson invariants $c_{U,2n-1}, \ldots, c_{U,n}$.

(iv) The polynomial $f_\infty Q^+(X)$ has all coefficients in the ring $F_{2^l}[\xi_1, \ldots, \xi_{2n}]$ where $l \geq 2$.

Proof. (i) The coefficients of $Q^-(X)$ are symplectic invariants and so, by knowledge of the invariants of the invariant ring for that case, these coefficients lie in the subring $F_{2^l}[\xi_1, \ldots, \xi_{2n}, c_{U,2n-1}, \ldots, c_{U,n}]$. Since by Theorem 6.2.4 there are $2^{2ln-1} - 2^{ln-1}$ quadratic forms of $-$type, the degree of $Q^-(X)$ is $2(2^{2ln-1} - 2^{ln-1}) = 2^{2ln} - 2^{ln}$. On the other hand, the least degree of an element of $F_{2^l}[\xi_1, \ldots, \xi_{2n}, c_{U,2n-1}, \ldots, c_{U,n}]$ which is quadratic in the Dickson invariants is deg $c_{U,2n-1}^2 = 2((2^l)^{2n} - (2^l)^{2n-1}) = 2^{2ln} + 2^{2ln-1} + 2^{2ln-2} + \cdots + 2^{2ln-(l-1)}$ and this is greater than the degree of $Q^-(X)$. Hence the coefficients of $Q^-(X)$ are, at worst, linear in the $c_{U,j}$.

(ii) We know that for each j, $f_\infty c_{U,j}$ belongs to $F_{2^l}[\xi_1, \ldots, \xi_{2n}]$ by Lemma 6.5.2. Part (i) says that the coefficients are linear in the $c_{U,j}$ and so the result follows.

(iii) The coefficients of $Q^+(X)$ are symplectic invariants and so, by our knowledge of the invariants of the invariant ring for that case, these coefficients lie in the subring $F_{2^l}[\xi_1, \ldots, \xi_{2n}, c_{U,2n-1}, \ldots, c_{U,n}]$. Since by Theorem 6.2.4 there are $2^{2ln-1} + 2^{ln-1}$ quadratic forms of $+$type, the degree of $Q^+(X)$ is $2(2^{2ln-1} + 2^{ln-1}) = 2^{2ln} + 2^{ln}$. On the other hand, the least degree of an element of

$F_{2^l}[\xi_1, \ldots, \xi_{2n}, c_{U,2n-1}, \ldots, c_{U,n}]$ which is quadratic in the Dickson invariants is $\deg c_{U,2n-1}^2 = 2((2^l)^{2n} - (2^l)^{2n-1}) = 2^{2ln} + 2^{2ln-1} + 2^{2ln-2} + \cdots + 2^{2ln-(l-1)}$ and this is greater than the degree of $Q^+(X)$. Hence the coefficients of $Q^+(X)$ are, at worst, linear in the $c_{U,j}$.

(iv) We know that for each j, $f_\infty c_{U,j}$ belongs to $F_{2^l}[\xi_1, \ldots, \xi_{2n}]$ by Lemma 6.5.2. Part (iii) says that the coefficients are linear in the $c_{U,j}$ and so the result follows.

□

Remark 6.6.4. A version of (iii) and (iv) is present in [24] when $l = 1$.

6.7 How to understand $\Omega_m(X)$

We shall study the image of $\Omega_m(X)$ in the polynomial ring $S[X]$ over our symmetric algebra S, using the specialization

$$F_{2^l}[X, \xi_1, \xi_2, \xi_3, \ldots] \to S[X]$$

defined by $X \mapsto X$ and $\xi_i \mapsto \xi_i$.

Theorem 6.7.1. *(i)* $\Omega_{2n}(X) = \sum_{i=0}^{2n} (\Lambda_{2n,i})^2 X^{(2^l)^i} + \delta$, *where* $\delta \in F_{2^l}[\xi_1, \xi_2, \ldots, \xi_{2n}]$.

(ii) In the ring S *we have* $\Omega_{2n}(X) = f_\infty^2 Q(X)$.

(iii) $\Omega_{2n}(X) = f_\infty^2 Q^-(X) Q^+(X)$, *and* $Q^-(X)$ *and* $Q^+(X)$ *are irreducible elements of the ring* $T^{(S_P(U,\ \bar{B}))}[X]$.

(iv) $f_\infty Q^-(X)$ *and* $f_\infty Q^+(X)$ *both belong to* $F_{2^l}[X, \xi_1, \ldots, \xi_{2n}]$.

Proof. (i) Looking at the standard expansion of the determinant H_{2n} we see first that the coefficient of any term involving a product of two or more of the diagonal entries will be divisible by 4. So these make zero contribution to Ω_{2n}. For $0 \leq i \leq 2n$, we see that the coefficient of $X^{(2^l)^i}$ in Ω_{2n} is precisely the determinant of the matrix $H_{2n,i}$ obtained by omitting the ith row and column (counting from 0 to $2n$) from NM_0N^T. This determinant is equal to $(\Lambda_{2n,i})^2$ as noted in the proof of Lemma 6.5.2.

(ii) Recall from Definition 6.6.2 that $Q(X) = \prod_{q \in C}(X+q)$ where $C = \{\xi_0 + x_0^2 + x^2 : x \in U^*\}$. Using Lemma 2.1.2, we know that the zero set of the polynomial $D'(X) = \sum_{i=0}^{2n} c_{U,i}^2 X^{(2^l)^i}$ is precisely $\{x^2 : x \in U^*\}$. (Note that $D'(x^2) = (D_U(x))^2$.) Thus

$$Q(X) = D'(X + \xi_0 + x_0^2) = D'(X) + D'(\xi_0 + x_0^2).$$

We claim that $\Omega_{2n}(X) = f_\infty^2 Q(X)$. First, it follows from Lemma 6.5.2 that $f_\infty^2 D'(X) = \sum_{i=0}^{2n} (\Lambda_{2n,i})^2 X^{(2^l)^i}$ and by part (i), this coincides with the part of $\Omega_{2n}(X)$ which involves X. Therefore

$$f_\infty^2 Q(X) + \Omega_{2n}(X)$$

does not involve X and to prove that it is zero it suffices to prove that

$$\Omega_{2n}(\xi_0 + x_0^2) = 0.$$

To this end we need to work over $\mathbb{Z}$ rather than F_{2^l} and we shall temporarily work with two abstract polynomials rings and the ring homomorphism as follows:

$$\alpha : \mathbb{Z}[X, \xi_1, \xi_2, \xi_3, \dots] \to \mathbb{Z}[x_1, x_2, \dots, x_{2n}]$$

where

$$\alpha(\xi_i) = \sum_{k=1}^{n} (x_{2k-1}^{(2^l)^i} x_{2k} + x_{2k-1} x_{2k}^{(2^l)^i})$$

and

$$\alpha(X) = \sum_{k=1}^{n} x_{2k-1} x_{2k}.$$

Consider the matrices N and $M_0 N^T$ and insert respectively a column and a row of zeros to make the matrices square. Then clearly they have determinant equal to zero, and further by using the Binomial Theorem we have a matrix equation:

$$\begin{bmatrix} 2y_0 & \xi_1 & \xi_2 & \cdots & \xi_{2n} \\ \xi_1 & 2y_1+4d_1 & \xi_1^{2^l}+2a_1 & \cdots & \xi_{2n-1}^{2^l}+2a_{2n-1} \\ \xi_2 & \xi_1^{2^l}+2a_1 & 2y_2+4d_2 & \cdots & \xi_{2n-2}^{(2^l)^2}+2b_{2n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{2n} & \xi_{2n-1}^{2^l}+2a_{2n-1} & \xi_{2n-2}^{(2^l)^2}+2b_{2n-2} & \cdots & 2y_{2n}+4d_{2n} \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_{2n} & 0 \\ x_1^{2^l} & x_2^{2^l} & x_3^{2^l} & \cdots & x_{2n}^{2^l} & 0 \\ x_1^{(2^l)^2} & x_2^{(2^l)^2} & x_3^{(2^l)^2} & \cdots & x_{2n}^{(2^l)^2} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{(2^l)^{2n}} & x_2^{(2^l)^{2n}} & x_3^{(2^l)^{2n}} & \cdots & x_{2n}^{(2^l)^{2n}} & 0 \end{bmatrix} \begin{bmatrix} x_2 & x_2^{2^l} & x_2^{(2^l)^2} & \cdots & x_2^{(2^l)^{2n}} \\ x_1 & x_1^{2^l} & x_1^{(2^l)^2} & \cdots & x_1^{(2^l)^{2n}} \\ x_4 & x_4^{2^l} & x_4^{(2^l)^3} & \cdots & x_4^{(2^l)^{2n}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{2n-1} & x_{2n-1}^{2^l} & x_{2n-1}^{(2^l)^2} & \cdots & x_{2n-1}^{(2^l)^{2n}} \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

where $y_i = (x_1x_2+\cdots+x_{2n-1}x_{2n})^{(2^l)^i}$ for $0 \le i \le 2n$ and $a_i, b_i, d_i \in \mathbb{Z}[x_1, x_2, \ldots, x_{2n}]$. Let L.H.S $= A$, then by using the multilinearity of determinants,

$$\det A \equiv \begin{vmatrix} 2y_0 & \xi_1 & \xi_2 & \cdots & \xi_{2n} \\ \xi_1 & 2y_1 & \xi_1^{2^l} & \cdots & \xi_{2n-1}^{2^l} \\ \xi_2 & \xi_1^{2^l} & 2y_2 & \cdots & \xi_{2n-2}^{(2^l)^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{2n} & \xi_{2n-1}^{2^l} & \xi_{2n-2}^{(2^l)^2} & \cdots & 2y_{2n} \end{vmatrix} \pmod 4.$$

Now from the right hand side of the above equation, we have $\det A = 0$. Therefore $\alpha(H_{2n}) \equiv 0 \bmod 4$ and hence $\alpha(\frac{1}{2}H_{2n}) \equiv 0 \bmod 2$. (Recall from the remarks preceding Definition 6.4.1 that H_{2n} is divisible by 2.) By definition, $\Omega_{2n}(X) := (\frac{1}{2}H_{2n}) \bmod 2$. Now the image of $\alpha(\frac{1}{2}H_{2n})$ under the map $\mathbb{Z} \to F_{2^l}$ is $\Omega_{2n}(\xi_0 + x_0^2)$ and hence $\Omega_{2n}(\xi_0 + x_0^2) = 0$ as required.

(iii) By part (ii), $\Omega_{2n}(X) = f_\infty^2 Q(X) = f_\infty^2 Q^-(X)Q^+(X)$. The quadratic Chern polynomials $Q^\pm(X)$ are irreducible as the symplectic group transitively permutes their factors.

(iv) Follows from Lemma 6.6.3 (ii) and (iv).

□

Remark 6.7.2. Note that in part (ii) of the above proof we temporarily work over $\mathbb{Z}$ rather than F_{2^l}. We multiply the two matrices and get another matrix. In [24] the authors use the fact that $(x+y)^2 = x^2 + y^2$ when they multiply the matrices which is only true when x and y are elements of finite fields of characteristic 2. As promised in the introduction, the proof of part (ii) here corrects this flaw.

References

[1] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2000.

[2] M.F. Atiyah and I.G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[3] S. Barnes. *Aspects of The Ring of Invariants of the Orthogonal Group over Finite Fields in Odd Characteristic*. PhD thesis, University of Glasgow, 2008.

[4] D.J. Benson. Polynomial invariants of finite groups. volume 190 of *London Mathematical Society Lecture Note Series*, pages x+118. Cambridge University Press, Cambridge, 1993.

[5] W. Bruns and J. Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[6] P. J. Cameron. Projective and polar spaces. volume 13 of *QMW Maths Notes*, pages viii+147. Queen Mary and Westfield College School of Mathematical Sciences, London, 1991.

[7] P.J. Cameron. *Introduction to algebra*. Oxford Science Publications. Oxford University Press, Oxford, 1998.

[8] D. Carlisle and P.H. Kropholler. Modular invariants of finite symplectic group, preprint. 1992.

[9] D. Carlisle and P.H. Kropholler. Rational invariants of certain orthogonal and unitary groups. *Bull. London Math. Soc.*, 24(1):57–60, 1992.

[10] L. Chiang and Y. C. Hung. The invariants of orthogonal group actions. *Bull. Austral. Math. Soc.*, 48(2):313–319, 1993.

[11] H. Chu. Orthogonal group actions on rational function fields. *Bull. Inst. Math. Acad. Sinica*, 16(2):115–122, 1988.

[12] H. Chu. Polynomial invariants of four-dimensional orthogonal groups. *Comm. Algebra*, 29(3):1153–1164, 2001.

[13] H. Chu. Polynomial invariant of finite orthogonal groups of finite characteristics, unpublished. 2007.

[14] H. Chu and S.Y Jow. Polynomial invariants of finite unitary groups. *J. Algebra*, 302(2):686–719, 2006.

[15] S. D. Cohen. Rational functions invariant under an orthogonal group. *Bull. London Math. Soc.*, 22(3):217–221, 1990.

[16] L.E. Dickson. A fundamental system of invariants of the general modular linear group with a solution of the form problem. *Trans. Amer. Math. Soc.*, 12(1):75–98, 1911.

[17] D.S. Dummit and R.M. Foote. *Abstract algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[18] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view towards algebraic geometry.

[19] W. Fulton. *Young tableaux*, volume 35 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1997. With applications to representation theory and geometry.

[20] L.C. Grove. *Classical groups and geometric algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[21] N. Jacobson. *Basic algebra. I.* W. H. Freeman and Co., San Francisco, Calif., 1974.

[22] I. Kaplansky. *Commutative rings*. Allyn and Bacon Inc., Boston, Mass., 1970.

[23] P.H. Kropholler. *Notes on Cohomology*. University of Glasgow, Scotland, UK, http://www.maths.gla.ac.uk/ phk/, 2011.

[24] P.H. Kropholler, S.M. Rajaei, and J. Segal. Invariant rings of orthogonal groups over $\mathbb{F}_2$. *Glasg. Math. J.*, 47(1):7–54, 2005.

[25] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[26] Y.L. Lin. The invariants of unitary group actions. Master's thesis, National Taiwan University, 1993.

[27] S. Lipschutz. *Theory and problems of linear algebra*. McGraw-Hill, Inc., 1968.

[28] M.J. Macleod. *Generalizing the Cohen Macaulay condition and other homological properties*. PhD thesis, University of Glasgow, 2010.

[29] H. Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[30] H. Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Translated from the Japanese by M. Reid.

[31] J.S. Milne. *Field and Galois theory*. Mathematics Site - J.S. Milne, http://www.jmilne.org/math/, 2003.

[32] M.D. Neusel. *The Invariants of the Symplectic Groups*. Texas Tech University, http://www.math.ttu.edu/ mneusel/writings.html, 1998.

[33] M.D. Neusel. *Invariant theory*, volume 36 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2007.

[34] M.D. Neusel and L. Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.

[35] S. Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[36] J.J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[37] J.P. Serre. *Local algebra*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. Translated from the French by Chee Whye Chin and revised by the author.

[38] D. Sharpe. *Rings and factorization*. Cambridge University Press, Cambridge, 1987.

[39] L. Smith. *Polynomial invariants of finite groups*, volume 6 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1995.

[40] R.P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (N.S.)*, 1(3):475–511, 1979.

[41] I. Stewart. *Galois Theory*. Chapman & Hall/CRC Mathematics. Chapman & Hall/CRC, Boca Raton, FL, third edition, 2004.

[42] C.A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[43] C.W. Wilkerson. A primer on the Dickson invariants. In *Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982)*, volume 19 of *Contemp. Math.*, pages 421–434, Providence, RI, 1983. Amer. Math. Soc.