Glasgow Math. J. **47** (2005) 7–54.
DOI: 10.1017/S0017089504002198. Printed in the United Kingdom

INVARIANT RINGS OF ORTHOGONAL GROUPS OVER $\mathbb{F}_2$

P. H. KROPHOLLER
Dept. of Mathematics, University of Glasgow, University Gardens, Glasgow G12 8QW
e-mail: p.h.kropholler@maths.gla.ac.uk

S. MOHSENI RAJAEI
Departement of Mathematics, Azzahra University, Vanak, Tehran, Iran
e-mail: rajaei@azzahra.ac.ir

and J. SEGAL
Stegemühlenweg 70, 37083 Göttingen
e-mail: joel@berlin.com

(Received 22 December, 2003; accepted 16 August, 2004)

Abstract. We determine the rings of invariants S^G where S is the symmetric algebra on the dual of a vector space V over $\mathbb{F}_2$ and G is the orthogonal group preserving a non-singular quadratic form on V. The invariant ring is shown to have a presentation in which the difference between the number of generators and the number of relations is equal to the minimum possibility, namely dim V, and it is shown to be a complete intersection. In particular, the rings of invariants computed here are all Gorenstein and hence Cohen-Macaulay.

2000 *Mathematics Subject Classification.* 13A50, 20G40.

1. Strategy for calculating invariants. Let S be the symmetric algebra on V^*, the dual of a finite dimensional vector space V. For any finite subgroup G of $GL(V)$ we can consider the invariant ring S^G. This article concerns explicit calculations of S^G which are described in §6. In very broad outline, the strategy for doing calculations comprises the following steps:

- Find some reasonably large but finite collection of invariants of G using a variety of methods.
- Consider the subring of T which they generate. If we found enough invariants in the first step then T will be S^G and we are done. The strategy cannot be doomed to failure because S^G is a finitely generated ring.
- Prove that $T = S^G$.

The last step may fail. If it does, then we hope to discover new invariants. We throw these in to the generating set, enlarge T and try again. The proof is easy enough:

- Show that S is integral over T.
- Show that T has the right field of fractions.
- Show that T is integrally closed.

Only the third item here causes any real concern. In fact, we shall be working on examples which are known *a priori* to be unique factorization domains and we'll establish this for our T as the route to integral closure. Over $\mathbb{F}_2$ invariant rings are always unique factorization domains by a result of Nakajima, see Corollary 3.9.3 of [**2**]. This is not true in odd characteristic as illustrated by the very simple example 1 of

Chapter 1 of [**13**]. It is also not true in general for fields of characteristic 2 which have more than two elements. The following elementary result turns out to be decisive in every case considered in this paper:

PROPOSITION 1.1. *Let R be a commutative Noetherian ring and suppose that α, β is a regular sequence in R such that*

(i) *the localization $R[\alpha^{-1}]$ is a unique factorization domain;*

(ii) *α generates a prime ideal in the ring $R[\beta^{-1}]$.*

Then R is a unique factorization domain.

Proof. First, α being a non-zero divisor, the map $R \to R[\alpha^{-1}]$ is injective and so we know that R is a domain. Since α is prime in $R[\beta^{-1}]$, the quotient $R[\beta^{-1}]/\alpha R[\beta^{-1}]$ is a domain. Now β is a non-zero-divisor modulo α and so the map $R/\alpha R \to R[\beta^{-1}]/\alpha R[\beta^{-1}]$ is injective. Therefore α generates a prime ideal in R, and this together with the fact that $R[\alpha^{-1}]$ is a unique factorization domain implies that R is a unique factorization domain. The last step requires the assumption that R is Noetherian, otherwise one might envisage a situation in which an element of R is repeatedly and infinitely divisible by α but becomes irreducible in $R[\alpha^{-1}]$. □

We are indebted to the referee for pointing out that the Noetherian assumption is necessary here. All the rings we consider are of course Noetherian. Alternatively, the Noetherian assumption can be disposed of when the ring R is $\mathbb{N}$-graded and α and β are homogeneous elements of positive degree. Again, this is the case in our applications. A similar result holds in which one replaces the term *unique factorization domain* by *integrally closed domain*. This version has much the same effect but does not depend on the Noetherian assumption.

2. Introduction. In this paper we shall focus attention on an odd-dimensional vector space V over the field $\mathbb{F}_2$ of two elements which is endowed with a non-singular quadratic form ξ_0. We write $S = S(V^*)$ for the symmetric algebra on the dual V^* of V. The symmetric algebra is the polynomial ring in any chosen basis of V^*, and it inherits a natural action of $GL(V)$. The orthogonal group of automorphisms of V which preserve ξ_0 is denoted by $O(V)$. Our main objective is to compute the ring of invariants of $O(V)$. The results extend work [**11**, **12**] of the second author on the rational invariants of orthogonal groups.

The reader familiar with quadratic forms in characteristic 2, the associated finite orthogonal groups, the rudiments of the mod 2 Steenrod algebra and the Dickson invariants for the general linear group may now wish to skip straight to §6 for a statement of results.

We begin with some remarks which apply to any non-zero vector space V over any field K. A quadratic form q is a function

$$q : V \to K$$

which satisfies the two conditions

- the polarization

$$b : V \times V \to K$$

defined by

$$b(u, v) = q(u + v) - q(u) - q(v)$$

is bilinear; and

- for all scalars λ and all $v \in V$,

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

The polarization b is always a symmetric form. If the characteristic of K 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 K has characteristic 2 then the polarization is an alternating form from which the quadratic form cannot be recovered. If $K = \mathbb{F}_2$, the case of interest in this paper, then the definition of quadratic form simplifies: a function $q : V \to \mathbb{F}_2$ such that

- the polarization

$$b : V \times V \to \mathbb{F}_2$$

defined by

$$b(u, v) = q(u + v) + q(u) + q(v)$$

is bilinear.

In this case, every alternating form arises as the polarization of 2^m different quadratic forms, where $m = \dim V$, and the symmetric forms which are not alternating never arise as polarizations. Thus polarization yields a map between quadratic forms and symmetric bilinear forms which is neither injective nor surjective.

3. The Steenrod Algebra and Chern polynomials. Henceforth we assume that V is a vector space over $\mathbb{F}_2$. The symmetric algebra $S = S(V^*)$ is naturally isomorphic to the cohomology ring $H^*(BV, \mathbb{F}_2)$ of the classifying space BV of the additive group V, drawing attention to the fact that S admits an unstable action of the Steenrod Algebra $\mathcal{A}_2$. The reader is referred to the books [**13**, **15**] for details about the Steenrod Algebra.

Here the matter is simple enough. The Steenrod algebra is an $\mathbb{F}_2$-algebra generated by elements Sq^i, for $i \geq 0$, called *Steenrod squares*. Sq^i is homogeneous of degree i.

3.1. *The action on S is determined by the following facts*:

- Sq^0 *acts as the identity operation on* S;
- Sq^1 *acts as a derivation on* S;
- *for all* $x \in V^*$, $Sq^1(x) = x^2$ *and* $Sq^n(x) = 0$ *for* $n \geq 2$;
- *the Cartan formula holds: for all s and t in S,*

$$Sq^n(st) = \sum_{i+j=n} (Sq^i s)(Sq^i t).$$

- *for any homogeneous element s of S of degree d,* $Sq^d(s) = s^2$ *and* $Sq^j(s) = 0$ *if* $j > d$.
- *The total Steenrod operation* $Sq^\bullet := Sq^0 + Sq^1 + Sq^2 + \cdots$ *acts as a ring endomorphism of S.*

Now suppose that $\mathfrak{S}$ is a non-empty subset of V^* which contains d elements. The *Chern polynomial* associated to $\mathfrak{S}$ is the polynomial

$$\prod_{x \in \mathfrak{S}} (X + x).$$

Let's write f_i for the coefficient of X^{d-i} so that

$$\prod_{x \in \mathfrak{S}} (X + x) = f_0 X^d + f_1 X^{d-1} + \cdots + f_d.$$

Then it is easy to see that

LEMMA 3.2. *For each i in the range* $0 \leq i \leq d$,

$$Sq^i(f_d) = f_d f_i.$$

This is a special case of the Wu formulae [**7**, **16**, **20**] for the action of the Steenrod algebra on the cohomology ring $H^*(BO, \mathbb{F}_2)$ of the classifying space for real vector bundles which carries the generic Stiefel-Whitney classes. Arguably the name "Stiefel-Whitney polynomial" would be more appropriate in this paper than our choice: Chern polynomial. On the other hand, in modular invariant theory the similarity between the characteristic 2 theory and the odd characteristic theory is close and we stick with the name Chern polynomial.

4. Quadratic forms over $\mathbb{F}_2$. Each element of the symmetric algebra S determines a function from V to $\mathbb{F}_2$ and in this way the homogeneous elements of degree two in S determine quadratic forms on V. Conveniently, it is the case that this correspondence between S_2 and the set of quadratic forms on V is a bijection. We identify quadratic forms with the corresponding elements of S_2.

LEMMA 4.1. *Let q and q′ be quadratic forms on V. Then the following are equivalent:*

(i) *q and q′ have the same polarization;*
(ii) $Sq^1(q) = Sq^1(q')$*;*
(iii) $q + q' = x^2$ *for some* $x \in V^*$.

Proof. The details of this easy lemma are left to the reader. Note that the Steenrod operation Sq^1 is determined by virtue of being a derivation such that $Sq^1(x) = x^2$ for all $x \in V^*$. □

Two alternating forms b and b' on V are *equivalent* iff there exists $g \in GL(V)$ such that $b'(u, v) = b(gu, gv)$ for all u, v. Alternating forms are determined up to equivalence by rank, and the rank is always even. Let b be an alternating form on V. The radical $\mathrm{Rad}(b)$ of b is defined to be

$$\{v \in V;\ b(v,) = 0\}.$$

If q is a quadratic form which polarizes to b then the radical $\mathrm{Rad}(q)$ of q is defined to be

$$\{v \in \mathrm{Rad}(b);\ q(v) = 0\}.$$

Since the restriction of q to $\mathrm{Rad}(b)$ is a linear functional, one finds that $\mathrm{Rad}(q)$ is either equal to $\mathrm{Rad}(b)$ or has codimension 1 in $\mathrm{Rad}(b)$. A quadratic form q is called *non-singular* if and only if $\mathrm{Rad}(q) = 0$.

We consider quadratic forms always in the presence of a fixed alternating form to which they polarize. 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 the *symplectic group*. Non-singular quadratic forms live on symplectic spaces. On a symplectic space, we say that two quadratic forms q and q' are *equivalent* iff there exists g in the symplectic group such that $q'(v) = q(gv)$ for all v.

On a non-zero even dimensional symplectic space there are two types of non-singular quadratic form up to equivalence, called $+$type and $-$type. In dimension $2n \geq 2$

- $2^{2n-1} + 2^{n-1}$ of these forms have $+$type,
- $2^{2n-1} - 2^{n-1}$ of these forms have $-$type.

These quadratic forms are also classified by the Arf invariant which is determined by Browder's democracy: the Arf invariant is the value of the quadratic form taken by a majority of vectors. The forms of $+$type have Arf invariant 0 and the forms of $-$type have Arf invariant 1.

If V is an odd dimensional symplectic space, then 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 each form having the same polarization is equal to $\xi_0 + x^2$ for some $x \in V^*$ and there are three kinds: the non-singular forms (all equivalent to ξ_0), the singular forms of $+$type, and the singular forms of $-$type.

In this case, the polarization b is degenerate and its radical contains a vector $e_0 \neq 0$. Correspondingly there is a subspace U^* of V^* of codimension one and the forms of non-singular type are exactly the forms $\xi_0 + x^2$ for $x \in U^*$.

If $\dim V = 2n + 1 \geq 3$ then

- 2^{2n} of these forms are non-singular, and each is equal to $\xi_0 + x^2$ for some $x \in V^*$ such that $\operatorname{Ker} x \supseteq \operatorname{Rad}(b)$;
- $2^{2n-1} + 2^{n-1}$ of these forms have $+$type, and each is equal to $\xi_0 + x^2$ for certain $x \in V^*$ such that $\operatorname{Ker} x \cap \operatorname{Rad}(b) = 0$;
- $2^{2n-1} - 2^{n-1}$ of these forms have $-$type, and each is equal to $\xi_0 + x^2$ for certain $x \in V^*$ such that $\operatorname{Ker} x \cap \operatorname{Rad}(b) = 0$.

Note that for a $+$ or $-$type form q, this implies that $q = \xi_0 + x^2$ is actually in $S(U^*)$. Note also that the Arf invariant is not defined for the non-singular forms.

The analysis of non-singular quadratic spaces can be made using Witt's Theorem:

THEOREM 4.2 (Witt's Theorem). *Let (V, q) be a non-singular quadratic space and let $f : U_1 \to U_2$ be an isometric isomorphism between two subspaces U_1 and U_2. Then f extends to an isometry of V.*

For example, suppose that V is a symplectic space of dimension $2n + 1$ with symplectic form b and U is the $2n$-dimensional quotient of V by the radical of b. Then any compatible quadratic form q of $-$type on V has the same radical and passes to a non-singular quadratic form on U. The one-dimensional subspaces of U fall into two kinds according as the form q vanishes or does not vanish on their non-zero vectors. By Witt's Theorem, the orthogonal group on U therefore has two orbits on the non-zero vectors of U. Since the polarization b is non-degenerate, it induces a natural isomorphism between U and its dual U^*, so the orthogonal group also has two orbits on the non-zero vectors in U^*. Thus there are two kinds of maximal subspace in U. For example, if $n = 2$ and

$$q = x_1^2 + x_1x_2 + x_2^2 + x_3x_4$$

on U then q has $-$type, and its restriction to the subspace $\operatorname{Ker} x_1$ is equivalent to

$$x_2^2 + x_3x_4$$

which is non-singular on the 3-dimensional space $\operatorname{Ker} x_1 \subset U$, whereas its restriction to $\operatorname{Ker} x_3$ is equivalent to

$$q = x_1^2 + x_1x_2 + x_2^2$$

which is singular of $-$type on $\operatorname{Ker} x_3$. Thus x_1 and x_3 lie in different orbits under the action of the orthogonal group preserving q. Since there are only two orbits, these are representative. Notice that there are therefore no maximal subspaces on which q restricts to a form of $+$type.

There is another way of describing the orbits on non-zero vectors x in U^*. They fall into different kinds according to the type of the quadratic form $q + x^2$. In the examples above, notice that $q + x_1^2$ has $+$type and $q + x_3^2$ has $-$type. In summary:

LEMMA 4.3. *If q is a form of $-$type on V and x is a non-zero element of U^* then $q + x^2$ has $-$type if and only if q restricts to a $-$type form on* $\operatorname{Ker} x$ *and $q + x^2$ has $+$type if and only if q restricts to a non-singular form on* $\operatorname{Ker} x$.

A similar result applies to forms q of $+$type: simply interchange $+$ and $-$ throughout this statement.

5. Definitions. In this section we state our definitions of symplectic and orthogonal groups and those of their representations that we consider.

Let n be a positive integer. Henceforth we suppose that V has dimension $2n + 1$ over $\mathbb{F}_2$ 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 the $\operatorname{Rad}(b)$.

The reader is referred to Cameron's notes [**4**] for the background to the following lemma and definition.

LEMMA 5.1. *It is possible to choose the e_i for $i \geq 1$ so that the matrix B with (i, j)-entry $B_{i,j} = b(e_i, e_j)$ is*

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

filled out with zeroes.

We write B_0 for the non-singular alternating matrix obtained by omitting the first row and column of B.

DEFINITION 5.2. (i) $O(V)$ denotes the (orthogonal) group of automorphisms of V which preserve the quadratic form ξ_0.

(ii) $Sp(V)$ denotes the (symplectic) group of automorphisms of V which preserve the alternating form b.

$$O(V) \subset Sp(V).$$

(iii) U denotes the quotient $V/\langle e_0 \rangle$. This space inherits the alternating form, but it does not inherit any natural quadratic form.

(iv) $Sp(U)$ denotes the (symplectic) group of automorphisms of U which preserve the inherited alternating form.

Let $x_0, \ldots, x_{2n}$ be the basis of V^* which is dual to our chosen basis of V. We remark that when the basis e_i is chosen in accordance with Lemma 5.1, then the quadratic form is given by

$$\xi_0 = x_0^2 + x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}.$$

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 $x_1, \ldots, x_{2n}$. Every symplectic automorphism of V induces a symplectic automorphism of U, and every symplectic automorphism of U arises this way. In this way there is a surjective homomorphism

$$Sp(V) \to Sp(U).$$

The kernel of this homomorphism consists of transvections: it is the elementary abelian 2-group of rank $2n$ comprising the linear automorphisms of V which fix e_0 and induce trivial action on U, and can be naturally identified with $\hom(U, \langle e_0 \rangle) \cong U^*$. The homomorphism between the symplectic groups restricts to an isomorphism

$$O(V) \cong Sp(U).$$

DEFINITION 5.3. The sequence $\xi_1, \xi_2, \xi_3, \ldots$ is defined recursively by

$$\xi_n = Sq^{2^{n-1}}(\xi_{n-1}).$$

When the basis e_i is chosen in accordance with Lemma 5.1, then

$$\xi_j = x_1^{2^j}x_2 + x_1x_2^{2^j} + x_3^{2^j}x_4 + x_3x_4^{2^j} + \cdots + x_{2n-1}^{2^j}x_{2n} + x_{2n-1}x_{2n}^{2^j}$$

for each $j \geq 1$.

In general, for $i \geq 1$, each ξ_i belongs to the symmetric algebra on U^* (i.e. it does not involve x_0) and is an invariant of $Sp(U)$. For each $i \geq 0$, ξ_i has degree $2^i + 1$. The following results are important:

LEMMA 5.4.

$$\begin{aligned} Sq^\bullet(\xi_0) &= \xi_0 + \xi_1 + \xi_0^2, \\ Sq^\bullet(\xi_1) &= \xi_1 + \xi_2 + \xi_1^2, \\ Sq^\bullet(\xi_i) &= \xi_i + \xi_{i-1}^2 + \xi_{i+1} + \xi_i^2 \qquad (i \geq 2). \end{aligned}$$

Proof. It is easy given that $Sq^\bullet$ is a ring homomorphism and $Sq^\bullet x = x + x^2$ for $x \in V^*$. □

COROLLARY 5.5. *For any j and any $m \geq 0$,*

- $Sq^j(\mathbb{F}_2[\xi_0, \ldots, \xi_m]) \subseteq \mathbb{F}_2[\xi_0, \ldots, \xi_{m+1}]$;
- $Sq^j(\mathbb{F}_2[\xi_1, \ldots, \xi_m]) \subseteq \mathbb{F}_2[\xi_1, \ldots, \xi_{m+1}]$.

DEFINITION 5.6. Elements $c_0, \ldots, c_{2n}$ of $S(U^*)$ are defined to be the unique elements of S such that

$$\prod_{x \in U^*} (X + x) = \sum_{j=0}^{2n} c_j X^{2^j}.$$

These are the Dickson invariants:

$$S(U^*)^{GL(U)} = \mathbb{F}_2[c_{2n-1}, \ldots, c_0].$$

We write $D(X)$ for the Dickson polynomial.

Notice that the Dickson polynomial is the Chern polynomial associated to the subset $\mathfrak{S} := U^*$. Using Lemma 3.2 we have that

LEMMA 5.7. *For $0 \leq i \leq 2n$,*

$$Sq^{2^{2n}-2^i}(c_0) = c_0 c_i$$

and $Sq^j(c_0)$ is zero in all other cases.

Dickson's original paper [**5**] introduced these invariants: for a more modern treatment see Wilkerson [**18**]. Crucially, $c_0 D(X)$ is equal to the determinant

$$\begin{vmatrix} X & x_1 & x_2 & x_3 & \ldots & x_{2n} \\ X^2 & x_1^2 & x_2^2 & x_3^2 & \ldots & x_{2n}^2 \\ X^4 & x_1^4 & x_2^4 & x_3^4 & \ldots & x_{2n}^4 \\ X^8 & x_1^8 & x_2^8 & x_3^8 & \ldots & x_{2n}^8 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ X^{2^{2n}} & x_1^{2^{2n}} & x_2^{2^{2n}} & x_3^{2^{2n}} & \ldots & x_{2n}^{2^{2n}} \end{vmatrix}.$$

Let C_0 denote the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_{2n} \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_{2n}^2 \\ x_1^4 & x_2^4 & x_3^4 & \ldots & x_{2n}^4 \\ x_1^8 & x_2^8 & x_3^8 & \ldots & x_{2n}^8 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{2^{2n-1}} & x_2^{2^{2n-1}} & x_3^{2^{2n-1}} & \ldots & x_{2n}^{2^{2n-1}} \end{pmatrix}.$$

Then C_0 has determinant c_0 and the matrix equation below simply expresses the fact that $D(x_i)$ vanishes for each i.

LEMMA 5.8.

$$C_0^T \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{2n-1} \end{pmatrix} = \begin{pmatrix} x_1^{2^{2n}} \\ x_2^{2^{2n}} \\ x_3^{2^{2n}} \\ \vdots \\ x_{2n}^{2^{2n}} \end{pmatrix}.$$

For later use, we write C for the $(2n+1) \times 2n$-matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_{2n} \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_{2n}^2 \\ x_1^4 & x_2^4 & x_3^4 & \dots & x_{2n}^4 \\ x_1^8 & x_2^8 & x_3^8 & \dots & x_{2n}^8 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{2^{2n-1}} & x_2^{2^{2n-1}} & x_3^{2^{2n-1}} & \dots & x_{2n}^{2^{2n-1}} \\ x_1^{2^{2n}} & x_2^{2^{2n}} & x_3^{2^{2n}} & \dots & x_{2n}^{2^{2n}} \end{pmatrix},$$

and we write $\widehat{C}$ for the $(2n+1) \times (2n+1)$-matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & \dots & x_{2n} \\ x_0^2 & x_1^2 & x_2^2 & x_3^2 & \dots & x_{2n}^2 \\ x_0^4 & x_1^4 & x_2^4 & x_3^4 & \dots & x_{2n}^4 \\ x_0^8 & x_1^8 & x_2^8 & x_3^8 & \dots & x_{2n}^8 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_0^{2^{2n}} & x_1^{2^{2n}} & x_2^{2^{2n}} & x_3^{2^{2n}} & \dots & x_{2n}^{2^{2n}} \end{pmatrix}.$$

LEMMA 5.9. *Suppose that $f_0, \dots, f_{2n}$ are elements of S with the property that for all i in the range 1 to $2n$,*

$$f_{2n} x_i^{2^{2n}} + f_{2n-1} x_i^{2^{2n-1}} + \cdots + f_2 x_i^4 + f_1 x_i^2 + f_0 x_i = 0.$$

Then

$$f_j = f_{2n} c_j$$

for all j.

Proof. The polynomial

$$f(X) = f_{2n} X^{2^{2n}} + f_{2n-1} X^{2^{2n-1}} + \cdots + f_2 X^4 + f_1 X^2 + f_0 X$$

vanishes on all x_i. The additivity of the Frobenius map enables us to conclude that $f(X)$ vanishes on any linear combination of the x_i: that is, $f(X)$ vanishes on U^*. Therefore $f(X)$ is divisible by the Dickson polynomial, and the result follows. □

6. Statement of Results for the Orthogonal Groups. We give a summary of the conclusions of the calculations.

Assume that $n \geq 2$ and that V is a $(2n+1)$-dimensional $\mathbb{F}_2$-space endowed with a non-singular quadratic form ξ_0. The cases $n \leq 1$ will be treated later and are quite elementary by comparison.

THEOREM 6.1. *Let $T^\dagger$ be an abstract polynomial ring on generators*

$$\xi_0, \ldots, \xi_{2n-2}, d_{2n-1}, \ldots, d_n$$

where ξ_i has degree $2^i + 1$ and d_j has degree $2^{2n-1} - 2^{j-1}$. Define the degree preserving map

$$T^\dagger \to S$$

by sending ξ_0 to the quadratic form of the same name, sending ξ_i to $Sq^{2^{i-1}} Sq^{2^{i-2}} \ldots Sq^1 \xi_0$ and sending d_j to the symmetric polynomial of the same degree in the set of vectors in V^* of $-$type (i.e. the elements x of V^* such that $\xi_0 + x^2$ has $-$type in S). Then the image of $T^\dagger$ in S is equal to the ring $S^{O(V)}$ of invariants of the orthogonal group of automorphisms preserving ξ_0. The kernel of the map is generated by a regular sequence of $n-2$ elements which are homogeneous of degrees $2^{2n-1} + 2^j$ for $1 \leq j \leq n-2$.

The $n-2$ relations can be expressed in matrix form as the sum of four column vectors not all of which are easily described at this stage. When they are expressed this way, we use an additional (redundant) generator ξ_{2n-1} and impose an additional relation at the beginning which amounts to an expression for ξ_{2n-1} in terms of the chosen generators:

$$\mathbf{S}_{n-1} \begin{pmatrix} d_n \\ \vdots \\ d_{2n-2} \end{pmatrix} + \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \end{pmatrix} + \sqrt{\left(\mathbf{L}'_n \mathbf{E}_n + \left(\mathbf{L}'_n \mathbf{K}_n + \mathbf{R}'_n\right) \mathbf{F}_n\right)} + \mathbf{G}_{n-1} d_{2n-1}.$$

Here, the matrices and vectors $\mathbf{S}_{n-1}$, $\mathbf{L}'_n$, $\mathbf{R}'_n$, $\mathbf{E}_n$, $\mathbf{F}_n$, $\mathbf{G}_{n-1}$ are defined subsequently and all involve only polynomials in the ξ's. Matrices $\mathbf{L}_n$, $\mathbf{R}_n$ are defined in the next section and the symbol $'$ above indicates the matrices obtained from these by deleting the first row. The matrix $\mathbf{K}_n$ and column vector $\mathbf{E}_n$ are also introduced in the next section. The column vector $\mathbf{F}_n$ arises as part of a connection (Lemma 13.8) between the symmetric polynomial invariants determined by $d_{2n-1}, \ldots, d_n$ and the Dickson invariants $c_{2n-1}, \ldots, c_n$ for the $2n$-dimensional quotient of V which inherits a natural alternating form. The matrix $\mathbf{S}_{n-1}$ has determinant equal to Λ_{2n-2}, a certain polynomial which is intimately related to the Dickson algebra for a vector space of dimension $2n-2$. The $\sqrt{\ }$ symbol here is used to indicate the matrix obtained by replacing each entry of the matrix to which it is applied by its square root. We shall see that every entry of $\left(\mathbf{L}'_n \mathbf{E}_n + \left(\mathbf{L}'_n \mathbf{K}_n + \mathbf{R}'_n\right) \mathbf{F}_n\right)$ is a square in $T^\dagger$.

The second of the four column vectors has ith entry $\xi_{2n-i}^{2^{i-1}}$ and the ith relation can be interpreted as saying that $\xi_{2n-i}^{2^{i-1}}$ can be expressed in terms of other generators and lower powers of ξ_{2n-i}. This relation cannot be deduced from any of the other relations.

The regular sequence of relations in $T^\dagger$ can be extended to a regular sequence of length equal to $3n-1$, the Krull dimension of $T^\dagger$, by taking the further $2n+1$ elements

$$\xi_0, \ldots, \xi_n, d_{2n-1}, \ldots, d_n.$$

The ring of invariants $S^{O(V)}$ is a complete intersection as described in §21 *of* [**8**].

Notice that we use symmetric polynomials arising from vectors of $-$type rather than $+$type to describe the invariants d_j. The reason for this is purely pragmatic: there are fewer vectors of $-$type.

In general for any symmetric algebra S on the dual of a finite vector space we know the following. The Hilbert series of any ring of invariants S^G has a Laurent expansion about $t=1$ which begins with

$$\frac{1}{|G|}\frac{1}{(1-t)^m} + \frac{r}{2|G|}\frac{1}{(1-t)^{m-1}} + \cdots$$

where m is the Krull dimension of S (i.e. the dimension of V) and r is determined by the reflections (i.e. elements fixing a hyperplane in V pointwise) using a ramification formula. The interpretation of the second coefficient in terms of reflections is the content of the Benson–Crawley-Boevey–Neeman theorem. This was first proved by Benson and Crawley-Boevey, see [**3**]. Subsequently, Neeman published a line of reasoning which uses the Riemann–Roch theorem, [**9**]. Evidence that the Riemann–Roch theorem is involved was observed much earlier in unpublished work [**17**] of Felipe Voloch.

Since our invariant ring is presented by means of a regular sequence the Hilbert series is very simply determined. The Hilbert series of the ring $T^\dagger$ is

$$\frac{1}{(1-t^2)(1-t^3)\cdots\left(1-t^{2^{2n-2}+1}\right)\cdot\left(1-t^{2^{2n-1}-2^{2n-2}}\right)\cdots\left(1-t^{2^{2n-1}-2^{n-1}}\right)}.$$

There is a contribution $(1-t^a)$ in the denominator for a generator of degree a. Each time a relation of degree b is imposed we simply multiply this Hilbert series by $(1-t^b)$ because the relation is a non-zero-divisor modulo its predecessors. We can therefore draw the following conclusions:

COROLLARY 6.2. *The ring of invariants $S^{O(V)}$ has Hilbert polynomial*

$$\frac{\left(1-t^{2^{2n-1}+2}\right)\cdots\left(1-t^{2^{2n-1}+2^{n-2}}\right)}{(1-t^2)(1-t^3)\cdots\left(1-t^{2^{2n-2}+1}\right)\cdot\left(1-t^{2^{2n-1}-2^{2n-2}}\right)\cdots\left(1-t^{2^{2n-1}-2^{n-1}}\right)}.$$

Proof. There is a contribution $(1-t^b)$ in the numerator for a relation of degree b. □

Noting that the Laurent power series expansion of

$$\frac{\prod_{i=1}^{k}(1-t^{b_i})}{\prod_{j=1}^{\ell}(1-t^{a_i})}$$

about $t=1$ begins

$$\frac{\prod b_j}{\prod a_i}\left(\frac{1}{(1-t)^m} + \frac{\sum(a_i-1)-\sum(b_j-1)}{2}\frac{1}{(1-t)^{m-1}} + \cdots\right)$$

where $m=\ell-k$, we can draw the following statistical data for our group $O(V)$:

COROLLARY 6.3. *The order of $O(V)$ is $2^{n^2}\prod_{j=1}^{n}(2^{2j}-1)$ and $O(V)$ contains $2^{2n}-1$ transvections. There is exactly one transvection corresponding to each hyperplane in V which contains the radical vector e_0, (i.e. e_0 is the non-zero vector in the polarization of ξ_0.)*

Proof. This follows directly from the Benson–Crawley-Boevey–Neeman theorem. Note that for a vector space over $\mathbb{F}_2$, the only possible reflections are transvections, and it is easy to see that any transvection in $O(V)$ must fix the radical vector e_0. Since only transvections are involved, the ramification formula for r in the Hilbert series simplifies to

$$r = \sum_W \alpha_W$$

where W runs through the hyperplanes of V and $\alpha_W = \log_2 |G_W|$ where G_W is the pointwise stabiliser of W. Since $O(V)$ acts transitively on the set of hyperplanes containing e_0, a simple counting argument tells us that there is exactly one transvection associated to each. □

We turn next to the ring of invariants $S(U^*)^{O^-}$ for an orthogonal group O^- which is the group of automorphisms of a $2n$-dimensional vector space U endowed with a quadratic form ξ_- of $-$type (Arf invariant 1).

THEOREM 6.4. *Let $T^\dagger$ be an abstract polynomial ring on generators*

$$\xi_0, \ldots, \xi_{2n-2}, d_{2n-1}, \ldots, d_{n+1}$$

where ξ_i has degree 2^i+1 and d_j has degree $2^{2n-1}-2^{j-1}$. Define the degree preserving map

$$T^\dagger \to S(U^*)$$

by sending ξ_0 to the quadratic form ξ_-, sending ξ_i to $Sq^{2^{i-1}}Sq^{2^{i-2}}\ldots Sq^1\xi_0$ and sending d_j to the symmetric polynomial of the same degree in the set of vectors in V^* of $-$type (i.e. the elements x of V^* such that $\xi_- + x^2$ has $-$type). Then the image of $T^\dagger$ in $S(U^*)$ is equal to the ring of invariants $S(U^*)^{O^-}$ of the orthogonal group of automorphisms preserving ξ_-. The kernel of the map is generated by a regular sequence of $n-2$ elements which are homogeneous of degrees $2^{2n-1}+2^j$ for $1 \le j \le n-2$.

The $n-2$ relations can be expressed in matrix form as the sum of three column vectors. When they are expressed this way, we use an additional (redundant) generator ξ_{2n-1} and impose an additional relation at the beginning which amounts to an expression for ξ_{2n-1} in terms of the chosen generators:

$$\mathbf{T}_{n-1}\begin{pmatrix} d_{n+1} \\ \vdots \\ d_{2n-1}\end{pmatrix} + \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}}\end{pmatrix} + \sqrt{\left(\mathbf{L}_n'\mathbf{E}_n + \left(\mathbf{L}_n'\mathbf{K}_n + \mathbf{R}_n'\right)\mathbf{F}_n\right)}.$$

The matrix $\mathbf{T}_{n-1}$ involves only the ξ's and has determinant equal to $\Omega^-_{2n-2}(\xi_-)$, a certain polynomial which is intimately related to the sets of quadratic forms of $-$type on spaces of dimensions $2n-2$ and $2n$. The second of the three column vectors has ith entry $\xi_{2n-i}^{2^{i-1}}$ and the ith relation can be interpreted as saying that in the ring S, $\xi_{2n-i}^{2^{i-1}}$ can be expressed in terms of other generators and lower powers of ξ_{2n-i}. This relation cannot be deduced from any of the other relations.

The regular sequence of relations in $T^\dagger$ can be extended to a regular sequence of length equal to $3n-1$, the Krull dimension of $T^\dagger$, by taking the further $2n+1$ elements

$$\xi_0, \ldots, \xi_n, d_{2n-1}, \ldots, d_{n+1}.$$

The ring of invariants $S(U^*)^{O^-}$ is a complete intersection.

We can read off corollaries about the Hilbert series as before.

COROLLARY 6.5. *The Hilbert series of the ring $S(U^*)^{O^-}$ is*

$$\frac{\left(1-t^{2^{2n-1}+2}\right)\cdots\left(1-t^{2^{2n-1}+2^{n-2}}\right)}{(1-t^2)(1-t^3)\cdots\left(1-t^{2^{2n-2}+1}\right)\cdot\left(1-t^{2^{2n-1}-2^{2n-2}}\right)\cdots\left(1-t^{2^{2n-1}-2^n}\right)}.$$

COROLLARY 6.6. *The order of O^- is $2^{n^2-n+1}(2^n+1)\prod_{j=1}^{n-1}(2^{2j}-1)$ and O^- contains $2^{2n-1}+2^{n-1}$ transvections. There is exactly one transvection corresponding to each hyperplane in U which is the kernel of a $+$type vector $x \in U^*$ (i.e. $\xi_- + x^2$ has $+$type.)*

Finally we have the groups of $+$type. Let U be a $2n$-dimensional vector space endowed with a quadratic form ξ_+ of $+$type (Arf invariant 0). Notice that we still use vectors of $-$type to describe the generators d_j even though this is the $+$type case!

THEOREM 6.7. *Let $T^\dagger$ be an abstract polynomial ring on generators*

$$\xi_0, \ldots, \xi_{2n-2}, d_{2n-1}, \ldots, d_n$$

where ξ_i has degree 2^i+1 and d_j has degree $2^{2n-1}-2^{j-1}$. Define the degree preserving map

$$T^\dagger \to S(U^*)$$

by sending ξ_0 to the quadratic form ξ_+, sending ξ_i to $Sq^{2^{i-1}}Sq^{2^{i-2}}\ldots Sq^1\xi_+$ and sending d_j to the symmetric polynomial of the same degree in the set of vectors in V^* of $-$type (i.e. the elements x of V^* such that $\xi_+ + x^2$ has $-$type). Then the image of $T^\dagger$ in $S(U^*)$ is equal to the ring of invariants $S(U^*)^{O^+}$ of the orthogonal group of automorphisms preserving ξ_+. The kernel of the map is generated by a regular sequence of $n-1$ elements which are homogeneous of degrees $2^{2n-1}+2^j$ for $1 \le j \le n-1$.

The $n-1$ relations can be expressed in matrix form as the sum of three column vectors. When they are expressed this way, we use an additional (redundant) generator ξ_{2n-1} and impose an additional relation at the beginning which amounts to an expression for ξ_{2n-1} in terms of the chosen generators:

$$\mathbf{M}_n\begin{pmatrix} d_n \\ \vdots \\ d_{2n-1}\end{pmatrix} + \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \\ \\ \xi_n^{2^{n-1}}\end{pmatrix} + \begin{pmatrix} \sqrt{\mathbf{L}'_n\mathbf{E}_n + \left(\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n\right)\mathbf{F}_n} \\ \\ \xi_n^{2^{n-1}} + f_n\end{pmatrix}.$$

The matrix $\mathbf{M}_n$ involves only polynomials in the ξ's and its determinant is $\Omega^+_{2n-2}(\xi_+)$, a certain polynomial which is intimately related to the sets of quadratic forms of $+$type on spaces of dimensions $2n-2$ and $2n$. The polynomial f_n is also a polynomial involving only

the ξ's. The second of the three column vectors has ith entry $\xi_{2n-i}^{2^{i-1}}$ and the ith relation can be interpreted as saying that in the ring S, $\xi_{2n-i}^{2^{i-1}}$ can be expressed in terms of other generators and lower powers of ξ_{2n-i}. This relation cannot be deduced from any of the other relations.

The regular sequence of relations in $T^\dagger$ can be extended to a regular sequence of length equal to $3n-1$, the Krull dimension of $T^\dagger$, by taking the further $2n$ elements

$$\xi_+, \ldots, \xi_{n-1}, d_{2n-1}, \ldots, d_n.$$

The ring of invariants $S(U^*)^{O^+}$ is a complete intersection.

COROLLARY 6.8. *The Hilbert series of the ring $S(U^*)^{O^+}$ is*

$$\frac{\left(1-t^{2^{2n-1}+2}\right)\cdots\left(1-t^{2^{2n-1}+2^{n-1}}\right)}{(1-t^2)(1-t^3)\cdots\left(1-t^{2^{2n-2}+1}\right)\cdot\left(1-t^{2^{2n-1}-2^{2n-2}}\right)\cdots\left(1-t^{2^{2n-1}-2^{n-1}}\right)}.$$

COROLLARY 6.9. *The order of O^+ is $2^{n^2-n+1}(2^n-1)\prod_{j=1}^{n-1}(2^{2j}-1)$ and O^+ contains $2^{2n-1}-2^{n-1}$ transvections. There is exactly one transvection corresponding to each hyperplane in U which is the kernel of a $-$type vector $x \in U^*$ (i.e. $\xi_+ + x^2$ has $-$type.)*

7. Connection with work of Domokos and Frenkel. There is a potentially interesting connection between our calculations and those in [**6**]. If $\overline{\mathbb{F}_2}$ denotes the algebraic closure of $\mathbb{F}_2$ then we can consider the space $V \otimes \overline{\mathbb{F}_2}$ and its coordinate ring $\overline{\mathbb{F}_2}[V] \cong S(V^*) \otimes \overline{\mathbb{F}_2}$. Here we can look at the invariants of the full orthogonal group, the subgroup of $GL(V \otimes \overline{\mathbb{F}_2})$ preserving the quadratic form on V. Then the only invariant is the quadratic form itself. In this context, Domokos and Frenkel work with invariants of several vectors, that is, they study the invariants in the coordinate ring of a direct sum $V \otimes \overline{\mathbb{F}_2} \oplus \cdots \oplus V \otimes \overline{\mathbb{F}_2}$ of several copies of V. This coordinate ring can be identified with the tensor product

$$\overline{\mathbb{F}_2}[V] \otimes \cdots \otimes \overline{\mathbb{F}_2}[V]$$

and one can now consider the $\mathbb{F}_2$-linear map to $\overline{\mathbb{F}_2}[V]$ given by

$$s_1 \otimes s_2 \otimes s_3 \otimes \ldots \mapsto s_1 s_2^2 s_3^4 \ldots.$$

Using this it can be seen that the invariants of several vectors for the algebraic group give rise to the invariants ξ_j for our finite group. This raises the possibility of extracting new information about invariants in our setting from the results of [**6**]. For examle, Domokos and Frenkel show how to define an invariant which distinguishes the orthogonal group from the special orthogonal group and it seems reasonable to expect that this will map to an element of S which distinguishes $O(V)$ from $SO(V)$: note that in characteristic 2, the determinant does not distinguish these groups. We do not carry through these investigations here. We thank Steve Donkin and Matias Domokos for drawing attention to this connection.

8. Invariants in the symplectic case. The invariant ring $S(U^*)^{Sp(U)}$ is known. This was first calculated by Carlisle and Kropholler. Useful accounts have been published

by Benson (see Section 8.3 of [**2**]) and Neusel [**10**]. We shall have considerable need of this knowledge.

PROPOSITION 8.1. *The ring $S(U^*)^{Sp(U)}$ is generated by $\xi_1, \dots, \xi_{2n-1}, c_{2n-1}, \dots, c_n$. This ring is a unique factorization domain. In terms of the stated generators, it has a presentation given by a regular sequence $r_1, \dots, r_{n-1}$.*

To understand the relations, observe first that on multiplying both sides of the matrix identity of Lemma 5.8 by $C_0 B_0$ we obtain the matrix identity

$$\begin{pmatrix} 0 & \xi_1 & \xi_2 & \xi_3 & \dots & \xi_{2n-1} \\ \xi_1 & 0 & \xi_1^2 & \xi_2^2 & \dots & \xi_{2n-2}^2 \\ \xi_2 & \xi_1^2 & 0 & \xi_1^4 & \dots & \xi_{2n-3}^4 \\ \xi_3 & \xi_2^2 & \xi_1^4 & 0 & \dots & \xi_{2n-4}^8 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{2n-1} & \xi_{2n-2}^2 & \xi_{2n-3}^4 & \xi_{2n-4}^8 & \dots & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{2n-1} \end{pmatrix} = \begin{pmatrix} \xi_{2n} \\ \xi_{2n-1}^2 \\ \xi_{2n-2}^4 \\ \xi_{2n-3}^8 \\ \vdots \\ \xi_1^{2^{2n-1}} \end{pmatrix}.$$

This matrix equation records $2n$ relations which hold in the ring $S(U^*)^{Sp(U)}$. The first of these provides a formula for ξ_{2n} in terms of lower degree ξ_i and the Dickson invariants, so telling us that ξ_{2n} may be omitted from the list of generators of $S(U^*)^{Sp(U)}$. The next $n-1$ of these are, in disguise, the relations $r_1, \dots, r_{n-1}$. More mysteriously, it turns out that the Dickson invariants $c_{n-1}, \dots, c_0$ of higher degree can all be expressed as linear combinations of the Dickson invariants $c_{2n-1}, \dots, c_n$ of lower degree with coefficients in the ring $\mathbb{F}_2[\xi_1, \dots, \xi_{2n-1}]$.

LEMMA 8.2. *There is an $n \times n$ matrix $\mathbf{K}_n$ such that*

$$\begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = \mathbf{K}_n \begin{pmatrix} c_n \\ \vdots \\ c_{2n-1} \end{pmatrix} + \mathbf{E}_n.$$

The entries of $\mathbf{K}_n$ and $\mathbf{E}_n$ are all expressible as polynomials in the ξ's. The top entry of the column vector $\mathbf{E}_n$ is a certain polynomial Λ_{2n} in $\xi_1, \dots, \xi_{2n-1}$ which we review in the next section and which is equal to the Dickson invariant c_0 in the ring S. The matrix $\mathbf{K}_n$ has zeroes on and above the anti-diagonal. The matrix and column vector are related by the recursive block matrix formula

$$\mathbf{K}_n = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ & & & \\ \mathbf{K}_{n-1}^{*2} & & & \mathbf{E}_{n-1}^{*2} \end{pmatrix}$$

where the notation $\mathbf{K}_{n-1}^{*2}$ denotes the matrix obtained by squaring every element of $\mathbf{K}_{n-1}$.

This was proved by induction, and the proof is recorded unaltered in the accounts of Benson and Neusel. It remains of some interest to acquire a conceptual insight into this aspect of the ring $S(U^*)^{Sp(U)}$. The key relations in the symplectic case are the first n equations from the matrix equation exhibited following Proposition 8.1. Partition the

matrix into four $n \times n$ blocks. We are only concerned with the two blocks at the top which we denote by $\mathbf{L}_n$ and $\mathbf{R}_n$. The relations can now be expressed in matrix form as

$$\mathbf{L}_n \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} + \mathbf{R}_n \begin{pmatrix} c_n \\ \vdots \\ c_{2n-1} \end{pmatrix} = \begin{pmatrix} \xi_{2n} \\ \vdots \\ \xi_{n+1}^{2^{n-1}} \end{pmatrix}$$

We now make the substitutions for the redundant Dickson invariants $c_{n-1}, \ldots, c_0$ using Lemma 8.2. We then have

8.3. The fundamental relations for the symplectic invariants $S(U^*)^{Sp(U)}$:

$$(\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n) \begin{pmatrix} c_n \\ \vdots \\ c_{2n-1} \end{pmatrix} = \begin{pmatrix} \xi_{2n} \\ \vdots \\ \xi_{n+1}^{2^{n-1}} \end{pmatrix} + \mathbf{L}_n\mathbf{E}_n.$$

Here, the first relation simply gives expression for ξ_{2n} in terms of other generators, so we can omit this relation and discard the redundant generator ξ_{2n}. The remaining $n-1$ relations are the relations $r_1, \ldots, r_{n-1}$ referred to in Proposition 8.1.

From here it is easy to establish the ring of invariants of $Sp(V)$.

LEMMA 8.4. *The ring of invariants of $Sp(V)$ is generated by $S(U^*)^{Sp(U)}$ together with the single additional element*

$$\eta := \prod_{x \in V^* \setminus U^*} x.$$

Abstractly this is a polynomial ring in one variable of degree 2^{2n} over $S(U^*)^{Sp(U)}$.

Proof. As we remarked following Definition 5.2 the natural surjection

$$Sp(V) \to Sp(U)$$

has kernel an elementary abelian 2-group E of transvections. This subgroup acts trivially on U^* and clearly also fixes η. Hence

$$S^E \supseteq \mathbb{F}_2[x_1, \ldots, x_{2n}, \eta],$$

and a simple Galois theoretic argument shows that equality holds. Now, the action of $Sp(V)$ on S induces an action of $Sp(U)$ on S^E. The new element η is fixed by $Sp(U)$ and the action of $Sp(U)$ on the polynomials in $x_1, \ldots, x_{2n}$ is simply the classical action studied by Carlisle and Kropholler. Hence the result follows. □

LEMMA 8.5. *The elements $\xi_0, \ldots, \xi_{2n}$ are algebraically independent.*

Proof. Since $\xi_1, \ldots, \xi_{2n}$ all belong to $S(U^*)$ while ξ_0 involves the additional variable x_0, we need only show that $\xi_1, \ldots, \xi_{2n}$ are algebraically independent elements of $S(U^*)$. The determinant of the Jacobian matrix $(\frac{\partial \xi_i}{\partial x_j})_{1 \le i,j \le 2n}$ is $\det C_0 = c_0 \neq 0$ and the result follows from Proposition 5.4.2 of [**2**]. □

By contrast, the elements $\xi_0, \ldots, \xi_{2n+1}$ are obviously not algebraically independent since they live in the ring S of Krull dimension $2n+1$ and they are $2n+2$ in number.

At the risk of causing untold confusion we shall bravely work on the assumption that the ring

$$\mathbb{F}_2[\xi_0, \xi_1, \xi_2, \dots]$$

really is an abstract polynomial ring in the stated generators. The reason why we can get away with this apparent travesty is that in any given situation we shall only be concerned with the ξ up to ξ_{2n}. On the other hand we shall be proving our results in many cases by induction on n.

9. 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

$$H_m = \begin{vmatrix} 2X & \xi_1 & \xi_2 & \xi_3 & \dots & \xi_m \\ \xi_1 & 2X^2 & \xi_1^2 & \xi_2^2 & \dots & \xi_{m-1}^2 \\ \xi_2 & \xi_1^2 & 2X^4 & \xi_1^4 & \dots & \xi_{m-2}^4 \\ \xi_3 & \xi_2^2 & \xi_1^4 & 2X^8 & \dots & \xi_{m-3}^8 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_m & \xi_{m-1}^2 & \xi_{m-2}^4 & \xi_{m-3}^8 & \dots & 2X^{2^m} \end{vmatrix}$$

This is the determinant of a symmetric matrix. On passing to the quotient ring

$$\mathbb{F}_2[X, \xi_1, \xi_2, \xi_3, \dots],$$

the matrix is alternating. Since 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 9.1. For each even integer $m \geq 0$, we write $\Omega_m(X)$ for the image of the polynomial $\frac{1}{2}H_m$ in $\mathbb{F}_2[X, \xi_1, \xi_2, \xi_3, \dots]$.

This observation has also been made by Domokos and Frenkel, see Proposition 4.11 of [**6**]. As an example, in case $m = 2$ we find that

$$\Omega_2(X) = \xi_1^2 X^4 + \xi_2^2 X^2 + \xi_1^4 X + \xi_1^3 \xi_2.$$

When m is odd, the image of H_m in $\mathbb{F}_2[X, \xi_1, \xi_2, \xi_3, \dots]$ is non-zero and does not involve X. In fact it is the square of a polynomial in $\mathbb{F}_2[\xi_1, \xi_2, \xi_3, \dots]$. The determinant of any alternating matrix over a commutative ring is a square; namely the square of the Pfaffian. The determinant of an alternating matrix over a commutative $\mathbb{F}_2$-algebra is more obviously square because the only contributing terms come from diagonally symmetric choices of elements from the matrix. So we make the definition

DEFINITION 9.2. For each even integer m, we write Λ_m for the square root of the image of the polynomial H_{m-1} in $\mathbb{F}_2[\xi_1, \xi_2, \xi_3, \dots]$, that is, the Pfaffian of the matrix defining H_{m-1}.

For example,

$$\begin{aligned}\Lambda_2 &= \xi_1\\ \Lambda_4 &= \xi_1^5+\xi_2^3+\xi_1^2\xi_3\\ \Lambda_6 &= \xi_5\xi_3^2\xi_1^4+\xi_5\xi_2^6+\xi_5\xi_1^{10}+\xi_4^3\xi_1^4+\xi_4^2\xi_3\xi_2^4\\ &\quad+\xi_4^2\xi_2\xi_1^8+\xi_4\xi_3^4\xi_2^2+\xi_4\xi_2^8\xi_1^2+\xi_3^7+\xi_3^4\xi_1^9\\ &\quad+\xi_3^2\xi_2^9+\xi_3\xi_1^{18}+\xi_2^{12}\xi_1+\xi_2^3\xi_1^{16}+\xi_1^{21}\end{aligned}$$

In general, Λ_{2n} has $\frac{(2n)!}{2^n n!}$ terms, this being the number of permutations in the symmetric group on $\{1, 2, \ldots, 2n\}$ which are products of n disjoint transpositions. If

$$(i_1\ i_2)(i_3\ i_4)\cdots(i_{2n-1}\ i_{2n})$$

is such a permutation then there is a corresponding contribution

$$\xi_{|i_1-i_2|}^{2^{\min\{i_1,i_2\}-1}}\xi_{|i_3-i_4|}^{2^{\min\{i_3,i_4\}-1}}\cdots\xi_{|i_{2n-1}-i_{2n}|}^{2^{\min\{i_{2n-1},i_{2n}\}-1}}.$$

For example, Λ_8 has 105 terms of which the leading term (giving ξ_7 the highest priority and ξ_1 the lowest) $\xi_7\xi_5^2\xi_3^4\xi_1^8$ arises from the contribution of the permutation

$$(1\ 8)(2\ 7)(3\ 6)(4\ 5).$$

10. How to understand Λ_m. Working in S, recall that the matrix C_0, defined in Section 5, has determinant equal to the Dickson invariant c_0.

The extended matrix C delivers a sequence of square matrices $D_0, D_1 \ldots, D_{2n-1}, D_{2n} = C_0$ where D_i is obtained by omitting the ith row of C. It is known that D_i has determinant c_0c_i.

As in Section 5, B_0 denotes the $2n \times 2n$ matrix with (i, j)-entry $b(e_i, e_j)$, $i, j \geq 1$. Then B_0 is a non-singular alternating matrix and so it has determinant 1. Moreover

$$C_0^TB_0C_0 = \begin{pmatrix} 0 & \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_{2n-1}\\ \xi_1 & 0 & \xi_1^2 & \xi_2^2 & \cdots & \xi_{2n-2}^2\\ \xi_2 & \xi_1^2 & 0 & \xi_1^4 & \cdots & \xi_{2n-3}^4\\ \xi_3 & \xi_2^2 & \xi_1^4 & 0 & \cdots & \xi_{2n-4}^8\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ \xi_{2n-1} & \xi_{2n-2}^2 & \xi_{2n-3}^4 & \xi_{2n-4}^8 & \cdots & 0 \end{pmatrix}$$

On taking determinants, noting that $\det B_0 = 1$, we find that

$$\det\left(C_0^TB_0C_0\right) = c_0^2$$

can be expressed as a polynomial in the $Sp(U)$-invariants $\xi_1, \ldots, \xi_{2n-1}$. As this matrix is clearly congruent to the matrix of H_{2n-1} modulo 2, it follows that $\Lambda_{2n} = c_0$ in S and that c_0 itself can be expressed in terms of the ξ_i.

Playing this game with C in place of C_0, we have

$$CB_0C^T = \begin{pmatrix} 0 & \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_{2n-1} & \xi_{2n} \\ \xi_1 & 0 & \xi_1^2 & \xi_2^2 & \cdots & \xi_{2n-2}^2 & \xi_{2n-1}^2 \\ \xi_2 & \xi_1^2 & 0 & \xi_1^4 & \cdots & \xi_{2n-3}^4 & \xi_{2n-2}^4 \\ \xi_3 & \xi_2^2 & \xi_1^4 & 0 & \cdots & \xi_{2n-4}^8 & \xi_{2n-3}^8 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \xi_{2n-1} & \xi_{2n-2}^2 & \xi_{2n-3}^4 & \xi_{2n-4}^8 & \cdots & 0 & \xi_1^{2^{2n}} \\ \xi_{2n} & \xi_{2n-1}^2 & \xi_{2n-2}^4 & \xi_{2n-3}^8 & \cdots & \xi_1^{2^{2n}} & 0 \end{pmatrix}$$

DEFINITION 10.1. We define polynomials $\Lambda_{2n,i}$ for each $n \geq 2$ and $0 \leq i \leq 2n$ by

$$\Lambda_{2n,i} = Sq^{2^{2n}-2^i}(\Lambda_{2n}).$$

LEMMA 10.2. (i) *For each i in the range $0 \leq i \leq 2n$, we have $\Lambda_{2n,i} = c_0c_i$. Each $\Lambda_{2n,i}$ can also be interpreted as Pfaffians coming from the appropriate $2n \times 2n$ matrix obtained by omitting a row and corresponding column from C^TB_0C.*

(ii) *Λ_{2n} belongs to the ring $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n-1}]$, and here it is irreducible and also linear in ξ_{2n-1}:*

$$\Lambda_{2n} = \xi_{2n-1}(\Lambda_{2n-2})^2 + \textit{ terms involving } \xi_1, \ldots, \xi_{2n-2}.$$

Moreover,

$$\Lambda_{2n,2n} = \Lambda_{2n},$$

and

$$\Lambda_{2n,0} = (\Lambda_{2n})^2.$$

(iii) *For $1 \leq i \leq 2n-1$, the polynomial $\Lambda_{2n,i}$ belongs to the ring $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$ and is linear in ξ_{2n}:*

$$\Lambda_{2n,i} = \xi_{2n}(\Lambda_{2n-2,i-1})^2 + \textit{ terms involving } \xi_1, \ldots, \xi_{2n-1}.$$

Moreover, $\Lambda_{2n,i}$ is not divisible by Λ_{2n} for these values of i.

Proof. (i) We noted above that $\Lambda_{2n} = c_0$. By Lemma 5.7 it follows that $\Lambda_{2n,i} = c_0c_i$.

(ii) The nature of Λ_{2n} as a polynomial in $\xi_1, \ldots, \xi_{2n-1}$ is easily deduced from its definition as the square root of a determinant. Since the symplectic group acts transitively on the vectors of $U^* \setminus \{0\}$, it follows that in the invariant ring, $\Lambda_{2n} = c_0$ is irreducible and hence Λ_{2n} is irreducible when viewed as a polynomial in the symplectic invariants ξ_i.

(iii) From Lemma 5.4 and its Corollary we know that when a Steenrod operation is applied to Λ_{2n} the only way in which ξ_{2n} can become involved is through the application

$$
\begin{aligned}
\Lambda_2 &= \xi_1\\
\Lambda_{2,1} &= \xi_2\\
\Lambda_{2,0} &= \xi_1^2\\
\Lambda_4 &= \xi_3\xi_1^2 + \xi_2^3 + \xi_1^5\\
\Lambda_{4,3} &= \xi_4\xi_1^2 + \xi_3^2\xi_2 + \xi_2^4\xi_1\\
\Lambda_{4,2} &= \xi_4\xi_2^2 + \xi_3^3 + \xi_1^9\\
\Lambda_{4,1} &= \xi_4\xi_1^4 + \xi_3\xi_2^4 + \xi_2\xi_1^8\\
\Lambda_{4,0} &= \xi_3^2\xi_1^4 + \xi_2^6 + \xi_1^{10}\\
\Lambda_6 &= \xi_5\xi_3^2\xi_1^4 + \xi_5\xi_2^6 + \xi_5\xi_1^{10} + \xi_4^3\xi_1^4 + \xi_4^2\xi_3\xi_2^4\\
&\quad + \xi_4^2\xi_2\xi_1^8 + \xi_4\xi_3^4\xi_2^2 + \xi_4\xi_2^8\xi_1^2 + \xi_3^7 + \xi_3^4\xi_1^9\\
&\quad + \xi_3^2\xi_2^9 + \xi_3\xi_1^{18} + \xi_2^{12}\xi_1 + \xi_2^3\xi_1^{16} + \xi_1^{21}\\
\Lambda_{6,5} &= \xi_6\xi_3^2\xi_1^4 + \xi_6\xi_2^6 + \xi_6\xi_1^{10} + \xi_5^2\xi_4\xi_1^4 + \xi_5^2\xi_3\xi_2^4\\
&\quad + \xi_5^2\xi_2\xi_1^8 + \xi_4^5\xi_2^2 + \xi_4^4\xi_3^3 + \xi_4^4\xi_1^9 + \xi_4\xi_3^8\xi_1^2\\
&\quad + \xi_3^{10}\xi_2 + \xi_3^8\xi_2^4\xi_1 + \xi_3\xi_2^{16}\xi_1^2 + \xi_2^{19} + \xi_2^{16}\xi_1^5\\
\Lambda_{6,4} &= \xi_6\xi_4^2\xi_1^4 + \xi_6\xi_3^4\xi_2^2 + \xi_6\xi_2^8\xi_1^2 + \xi_5^3\xi_1^4 + \xi_5^2\xi_3^5\\
&\quad + \xi_5^2\xi_2^9 + \xi_5\xi_4^4\xi_2^2 + \xi_5\xi_3^8\xi_1^2 + \xi_4^6\xi_3 + \xi_4^4\xi_2^8\xi_1\\
&\quad + \xi_4^2\xi_3^8\xi_2 + \xi_3^{12}\xi_1 + \xi_3\xi_1^{34} + \xi_2^3\xi_1^{32} + \xi_1^{37}\\
\Lambda_{6,3} &= \xi_6\xi_4^2\xi_2^4 + \xi_6\xi_3^6 + \xi_6\xi_1^{18} + \xi_5^3\xi_2^4 + \xi_5^2\xi_4\xi_3^4\\
&\quad + \xi_5^2\xi_2\xi_1^{16} + \xi_5\xi_4^4\xi_3^2 + \xi_5\xi_2^{16}\xi_1^2 + \xi_4^7 + \xi_4^4\xi_1^{17}\\
&\quad + \xi_4^2\xi_2^{17} + \xi_4\xi_1^{34} + \xi_3^4\xi_2^{16}\xi_1 + \xi_3^2\xi_2\xi_1^{32} + \xi_2^4\xi_1^{33}\\
\Lambda_{6,2} &= \xi_6\xi_4^2\xi_1^8 + \xi_6\xi_3^2\xi_2^8 + \xi_6\xi_2^2\xi_1^{16} + \xi_5^3\xi_1^8 + \xi_5^2\xi_4\xi_2^8\\
&\quad + \xi_5^2\xi_3\xi_1^{16} + \xi_5\xi_3^{10} + \xi_5\xi_2^{18} + \xi_4^3\xi_3^8 + \xi_4^2\xi_3\xi_2^{16}\\
&\quad + \xi_4\xi_2^2\xi_1^{32} + \xi_3^8\xi_1^{17} + \xi_3^3\xi_1^{32} + \xi_2^{24}\xi_1 + \xi_1^{41}\\
\Lambda_{6,1} &= \xi_6\xi_3^4\xi_1^8 + \xi_6\xi_2^{12} + \xi_6\xi_1^{20} + \xi_5\xi_4^4\xi_1^8 + \xi_5\xi_3^8\xi_2^4\\
&\quad + \xi_5\xi_2^{16}\xi_1^4 + \xi_4^5\xi_2^8 + \xi_4^4\xi_3\xi_1^{16} + \xi_4\xi_3^{12} + \xi_4\xi_1^{36}\\
&\quad + \xi_3^8\xi_2\xi_1^{16} + \xi_3^5\xi_2^{16} + \xi_3\xi_2^4\xi_1^{32} + \xi_2^{25} + \xi_2\xi_1^{40}
\end{aligned}
$$

Figure 1. Examples of the $\Lambda_{2n,i}$

of $Sq^{2^{2n-1}}$ to ξ_{2n-1}, and taking this together with the Cartan formula, we calculate

$$
\begin{aligned}
\Lambda_{2n,i} &= Sq^{2^{2n}-2^i}\Lambda_{2n}\\
&= Sq^{2^{2n}-2^i}\left(\xi_{2n-1}\Lambda_{2n-2,i-1}^2 + \text{ terms involving } \xi_1,\dots,\xi_{2n-2}\right)\\
&= Sq^{2^{2n-1}}\xi_{2n-1}\cdot Sq^{2^{2n-1}-2^i}\left(\Lambda_{2n-2,i-1}^2\right) + \text{ terms involving } \xi_1,\dots,\xi_{2n-1}\\
&= \xi_{2n}\cdot\left(Sq^{2^{2n-2}-2^{i-1}}\Lambda_{2n-2,i-1}\right)^2 + \text{ terms involving } \xi_1,\dots,\xi_{2n-1}\\
&= \xi_{2n}\Lambda_{2n-2,i-1}^2 + \text{ terms involving } \xi_1,\dots,\xi_{2n-1}.
\end{aligned}
$$

The last remarks now follow easily. □

Examples of the $\Lambda_{2n,i}$ are given in Figure 1.

We are indebted to the referee for correcting our original formulation of the following Lemma. As now stated, it is just what is required for subsequent application in the proof of 14.4.

LEMMA 10.3. *Let* $1 \leq i \leq 2n-1$. *Let* $J_i = \{s \in \mathbb{F}_2[\xi_0, \ldots, \xi_{2n}];\ sc_i \in \mathbb{F}_2[\xi_0, \ldots, \xi_{2n}]\}$. *Then* J_i *is the principal ideal of* $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n}]$ *generated by* Λ_{2n}.

Proof. Fix i. Let $t \in J_i$. Then we have $t \cdot \Lambda_{2n.i} = t \cdot c_0 c_i = t c_i \cdot \Lambda_{2n}$ and this is an equation in $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n}]$. Since Λ_{2n} does not divide $\Lambda_{2n,i}$, it must divide t. □

LEMMA 10.4. (i) *If* $s \in S$ *has the property that* s^2 *can be expressed as a polynomial in at most* $2n$ *of* $\xi_0, \ldots, \xi_{2n}$, *then* s *itself is a polynomial generated by the same* ξ_i.

(ii) *If* f *is a polynomial of degree* 2^{2n+1} *in* $F_2[\xi_0, \ldots, \xi_{2n}]$ *which is a square in the ambient ring* S *and which involves* ξ_{2n} *then* $\frac{\partial f}{\partial \xi_i} = c_0 c_i$ *for each* i *in the range* 0 *to* $2n$.

Proof. (i) An element f of S is a square if and only if

$$\frac{\partial f}{\partial x_i} = 0$$

for each i in the range 0 to $2n$. In the light of the first part of this lemma, we also know that if f belongs to the subring $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n}]$ then f is intrinsically a square within this ring if and only if

$$\frac{\partial f}{\partial \xi_i} = 0$$

for each i in the range 0 to $2n$. The transition between these two conditions is made via the Jacobian identity

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \\ \frac{\partial f}{\partial x_3} \\ \vdots \\ \frac{\partial f}{\partial x_{2n}} \end{pmatrix} = \begin{pmatrix} \frac{\partial \xi_0}{\partial x_0} & \frac{\partial \xi_1}{\partial x_0} & \frac{\partial \xi_2}{\partial x_0} & \frac{\partial \xi_3}{\partial x_0} & \cdots & \frac{\partial \xi_{2n}}{\partial x_0} \\ \frac{\partial \xi_0}{\partial x_1} & \frac{\partial \xi_1}{\partial x_1} & \frac{\partial \xi_2}{\partial x_1} & \frac{\partial \xi_3}{\partial x_1} & \cdots & \frac{\partial \xi_{2n}}{\partial x_1} \\ \frac{\partial \xi_0}{\partial x_2} & \frac{\partial \xi_1}{\partial x_2} & \frac{\partial \xi_2}{\partial x_2} & \frac{\partial \xi_3}{\partial x_2} & \cdots & \frac{\partial \xi_{2n}}{\partial x_2} \\ \frac{\partial \xi_0}{\partial x_3} & \frac{\partial \xi_1}{\partial x_3} & \frac{\partial \xi_2}{\partial x_3} & \frac{\partial \xi_3}{\partial x_3} & \cdots & \frac{\partial \xi_{2n}}{\partial x_3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \xi_0}{\partial x_{2n}} & \frac{\partial \xi_1}{\partial x_{2n}} & \frac{\partial \xi_2}{\partial x_{2n}} & \frac{\partial \xi_3}{\partial x_{2n}} & \cdots & \frac{\partial \xi_{2n}}{\partial x_{2n}} \end{pmatrix} \begin{pmatrix} \frac{\partial f}{\partial \xi_0} \\ \frac{\partial f}{\partial \xi_1} \\ \frac{\partial f}{\partial \xi_2} \\ \frac{\partial f}{\partial \xi_3} \\ \vdots \\ \frac{\partial f}{\partial \xi_{2n}} \end{pmatrix}.$$

The Jacobian matrix is equal to

$$B\widehat{C}^T.$$

Hence, if f is a square in S then the Jacobian identity tells us that for each i in the range 1 to $2n$,

$$\frac{\partial f}{\partial \xi_{2n}} x_i^{2^{2n}} + \frac{\partial f}{\partial \xi_{2n-1}} x_i^{2^{2n-1}} + \cdots + \frac{\partial f}{\partial \xi_1} x_i^2 + \frac{\partial f}{\partial \xi_0} x_i = 0.$$

From Lemma 5.9 we deduce that

$$\frac{\partial f}{\partial \xi_i} = \frac{\partial f}{\partial \xi_{2n}} c_i$$

for each $i \geq 0$. The hypotheses here guarantee that there is at least one choice of i for which $\frac{\partial f}{\partial \xi_i} = 0$ and the above equations now show that all $\frac{\partial f}{\partial \xi_i}$ vanish. Thus f is an intrinsic square as required.

(ii) From the proof of the last part, we know that $\frac{\partial f}{\partial \xi_i} = \frac{\partial f}{\partial \xi_{2n}} c_i$. Multiplying both sides of this equation by $c_0 = \Lambda_{2n}$ in S, recalling that $\Lambda_{2n,i} = c_0 c_i$, gives an equality in $F_2[\xi_0, \ldots, \xi_{2n}]$:

$$\Lambda_{2n} \frac{\partial f}{\partial \xi_i} = \frac{\partial f}{\partial \xi_{2n}} \Lambda_{2n,i}.$$

Since f involves ξ_{2n} and has degree less than that of ξ_{2n}^2 we know that it is linear in ξ_{2n} and that $\frac{\partial f}{\partial \xi_{2n}}$ is the coefficient of ξ_{2n}. Since Λ_{2n} does not divide $\Lambda_{2n,i}$ unless $i = 0$ or $2n$ we deduce that Λ_{2n} divides $\frac{\partial f}{\partial \xi_{2n}}$ and on grounds of degree, the result follows. □

11. The Chern Polynomials. In this section we define Chern polynomials whose coefficients can be plainly seen to be invariants of the orthogonal group $O(V)$ and "quadratic Chern polynomials" whose coefficients are plainly invariants of the symplectic group $Sp(U)$.

DEFINITION 11.1. 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 $A = A^+ \cup A^-$. Note that $A = V^* \setminus U^*$. Polynomials $P^+(t)$ and $P^-(t)$ in the polynomial ring $S[t]$ in one variable t of degree 1 are defined as follows:

$$P^+(t) := \prod_{x \in A^+} (t + x), \qquad P^-(t) := \prod_{x \in A^-} (t + x),$$

$$P(t) := \prod_{x \in A} (t + x).$$

We define n particular invariants $d_{2n-1}, \ldots, d_n$ by picking certain coefficients of $P^-(t)$:

$$d_j \textit{ is the coefficient of } P^-(t) \textit{ of degree } 2^{2n-1} - 2^{j-1}$$

for j in the range $n \leq j \leq 2n - 1$.

The orthogonal group $O(V)$ 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 $S^{O(V)}$. Note also that $P(t) = P^+(t)P^-(t)$.

The quadratic Chern polynomials are closely related:

DEFINITION 11.2. Let B^+ be the set of all quadratic forms on V of +type and B^- the set of all of −type. Let $B = B^+ \cup B^-$. Note that the elements of B belong to $S(U^*)$. Note that, from the discussion in §4 we know that $B = \{\xi_0 + x_0^2 + x^2;\ x \in U^*\}$. We define quadratic Chern polynomials $Q^+(X)$, $Q^-(X)$ and $Q(X)$ in the polynomial ring $S[X]$ in one variable X of degree 2 as follows:

$$Q^+(X) := \prod_{q \in B^+} (X + q), \qquad Q^-(X) := \prod_{q \in B^-} (X + q),$$
$$Q(X) := \prod_{q \in B} (X + q).$$

The symplectic group $Sp(U)$ permutes the elements of B^+ and B^-. Thus the coefficients of $Q^+(X)$ and $Q^-(X)$ are invariants of the symplectic group $Sp(V)$. Note also that $Q(X) = Q^+(X)Q^-(X)$.

We'll begin by illustrating these polynomials in the low dimensional cases:

EXAMPLE 11.3. The Case $n = 1$ and $\dim V = 3$.

If $n = 1$ then

$$Q^+(X) = X^3 + c_1 X^2 + \xi_1^2,$$
$$Q^-(X) = X + c_1.$$

In this case $c_1 = x_1^2 + x_1 x_2 + x_2^2$ happens to be the unique quadratic from of −type, and we also have the relation $c_0 = \xi_1$. Thus Q^+ is also given by

$$Q^+(X) = X^3 + c_1 X^2 + c_0^2,$$

reflecting the coincidence

$$Sp(U) = GL(U).$$

The invariant ring $S(U^*)^{Sp(U)}$ is generated by $\xi_1 = c_0$ and c_1: it is the ring of Dickson invariants.

Further, with respect to a suitable basis, $\xi_0 = x_0^2 + x_1 x_2$ and

$$\begin{aligned} P^+(t) &= t^3 + (x_0 + x_1 + x_2)t^2 + \xi_0 t + \xi_0(x_0 + x_1 + x_2) + \xi_1, \\ &= t^3 + d_1 t^2 + \xi_0 t + \xi_0 d_1 + \xi_1, \\ P^-(t) &= t + x_0 + x_1 + x_2, \\ &= t + d_1. \end{aligned}$$

The ring $S^{O(V)}$ is a polynomial ring with generators $x_0 + x_1 + x_2$, ξ_0 and ξ_1. In fact $O(V)$ is isomorphic to the symmetric group on 3 letters and its action on V permutes the basis $e_1, e_2, e_0 + e_1 + e_2$. On V^*, it permutes the dual basis $x_0 + x_1, x_0 + x_2, x_0$, and the invariants $x_0 + x_1 + x_2$, ξ_0 and $\xi_1 + \xi_0 d_1$ are the corresponding elementary symmetric polynomials.

EXAMPLE 11.4. The Case $n = 2$ and $\dim V = 5$.

If $n = 2$ then

$$\begin{aligned}
Q^+(X) &:= X^{10} + \xi_1^2 X^7 + (c_3 + \xi_1\xi_2)X^6 + \xi_2^2 X^5 \\
&\quad + \left(c_2 + \xi_1\xi_3 + \xi_1^4\right)X^4 + \xi_1^2\xi_2^2 X^2 + \xi_1^6 X + \left(\xi_1^4 c_3 + \xi_1^5\xi_2 + \xi_2^4\right) \\
Q^-(X) &:= X^6 + \xi_1^2 X^3 + (c_3 + \xi_1\xi_2)X^2 + \xi_2^2 X + (c_2 + \xi_1\xi_3)
\end{aligned}$$

We have also computed the polynomials $P^-(t)$ and $P^+(t)$ in this case, at least in terms of the two coefficients d_3, d_2 of $P^-(t)$. We have

$$\begin{aligned}
P^-(t) &= t^6 + \xi_0 t^4 + \xi_1 t^3 + d_3 t^2 + (\xi_2 + \xi_1\xi_0)t + d_2, \\
P^+(t) &= t^{10} + \xi_0 t^8 + \xi_1 t^7 + \left(d_3 + \xi_0^2\right)t^6 + (\xi_2 + \xi_1\xi_0)t^5 + \left(d_2 + \xi_1^2 + \xi_0^3\right)t^4 + \xi_1\xi_0^2 t^3 \\
&\quad + \left(\xi_0^2 d_3 + \xi_2\xi_1\right)t^2 + \left(\xi_2\xi_0^2 + \xi_1\xi_0^3 + \xi_1^3\right)t + \left(\xi_0^2 d_2 + \xi_1^2 d_3 + \xi_2^2 + \xi_2\xi_1\xi_0\right).
\end{aligned}$$

In this case there are 6 quadratic forms of minus type and so $Q^-(X)$ has degree 12. Since the ring of invariants of $Sp(U)$ is generated by $\xi_1, \xi_2, \xi_3, c_3, c_2$ subject to the single relation

$$\xi_1^2 c_2 + \xi_2^2 c_3 + \xi_1^3\xi_3 + \xi_1\xi_2^3 + \xi_3^2 + \xi_1^6 = 0,$$

we see that there is no ambiguity in expressing the coefficients of Q^- as polynomials in $\xi_1, \xi_2, \xi_3, c_3, c_2$. There are the following expressions for the other two Dickson invariants and for ξ_4 in terms of the minimal generating set.

$$\begin{aligned}
c_1 &= \xi_1^2 c_3 + \xi_3\xi_2 + \xi_2\xi_1^3, \\
c_0 &= \Lambda_4, \\
\xi_4 &= \left(\xi_3 + \xi_1^3\right)c_3 + \xi_2 c_2 + \xi_3\xi_2\xi_1 + \xi_2\xi_1^4.
\end{aligned}$$

When we introduce the orthogonal invariants d_3 and d_2 we find that

$$\begin{aligned}
c_3 &= d_3^2 + \xi_2\xi_1 + \xi_1^2\xi_0 + \xi_0^4 \\
c_2 &= d_2^2 + \xi_0^2 d_3^2 + \xi_3\xi_1 + \xi_2^2\xi_0 \\
\xi_3 &= \xi_1 d_2 + (\xi_2 + \xi_1\xi_0)d_3 + \xi_2\xi_0^2 + \xi_1^3
\end{aligned}$$

The orthogonal group $O(V)$ has invariant ring generated by $\xi_0, \xi_1, \xi_2, d_3, d_2$. Note that in this case, $O(V)$ is isomorphic to the symmetric group on 6 letters and so admits an action on a 6 dimensional space permuting a basis. We can then take V to be the 5 dimensional space consisting of the zero-sum vectors in the chosen basis and this gives the present representation of $O(V)$.

LEMMA 11.5. *The following identities hold in $S[t]$:*

$$\begin{aligned}
(P^+(t))^2 &= Q^+(t^2 + \xi_0) \\
(P^-(t))^2 &= Q^-(t^2 + \xi_0) \\
P(t) = P^-(t)P^+(t) &= D(t + x_0) = D(t) + D(x_0)
\end{aligned}$$

Proof. For the first two equalities, note that

$$\begin{aligned}(P^{\pm}(t))^2 &= \left(\prod_{x\in A^{\pm}}(t+x)\right)^2\\ &= \prod_{x\in A^{\pm}}(t^2+x^2)\\ &= \prod_{q\in B^{\pm}}(t^2+\xi_0+q)\\ &= Q^{\pm}(t^2+\xi_0)\end{aligned}$$

as $q \in B^{\pm}$ precisely when $q = \xi_0 + x^2$ with $x \in A^{\pm}$.

For the third,

$$\begin{aligned}P^-(t)P^+(t) &= \left(\prod_{x\in A^-}(t+x)\right)\left(\prod_{x\in A^+}(t+x)\right)\\ &= \prod_{x\in A}(t+x)\\ &= \prod_{x\in U^*}(t+x_0+x)\\ &= D(t+x_0).\end{aligned}$$

Further $D(X)$ is a polynomial in powers of 2, so is additive. □

LEMMA 11.6. (i) *The coefficients of $Q^-(X)$ belong to the subring of S generated by*

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

Moreover, they are linear in the Dickson invariants $c_{2n-1}, \ldots, c_n$.

(ii) *The polynomial $c_0Q^-(X)$ has all coefficients in the ring $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$.*

(iii) *The coefficients of $Q^+(X)$ belong to the subring of S generated by*

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

Moreover, the only conceivable terms which are not linear in the Dickson invariants are terms involving c_{2n-1}^2.

(iv) *The polynomial $c_0^2Q^+(X)$ has all coefficients in the ring $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$.*

(v) *The squares of the coefficients of $P^-(t)$ and of $P^+(t)$ belong to the subring of S generated by $\mathbb{F}_2[\xi_0, \xi_1, \ldots, \xi_{2n-1}, c_{2n-1}, \ldots, c_n]$.*

Proof. (i) The coefficients of Q^- are symplectic invariants and so, using our knowledge of the invariant ring for that case, Proposition 8.1, these coefficients lie in the subring $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n-1}, c_{2n-1}, \ldots, c_n]$. Since there are $2^{2n-1} - 2^{n-1}$ quadratic forms of $-$type, the degree of Q^- is $2(2^{2n-1} - 2^{n-1}) = 2^{2n} - 2^n$. On the other hand, the least degree of an element of $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n-1}, c_{2n-1}, \ldots, c_n]$ which is quadratic in the Dickson invariants is $\deg c_{2n-1}^2 = 2^{2n}$ and this is greater than the degree of Q^-. Hence the coefficients of Q^- are at worst linear in the c_j.

(ii) We know that for each j, c_0c_j belongs to $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$ by Lemma 10.2(i). Part (i) here says that the coefficients are linear in the c_j and so the result follows.

(iii) As in (i) we can use Proposition 8.1. For $n = 1$ or 2 we can see from the examples following Definition 11.2 that the result holds. For $n \geq 3$, the degree argument of

(i) yields only the weaker stated result because there are more $(2^{2n-1} + 2^{n-1})$ quadratic forms of $+$type.

(iv) Again, Lemma 10.2(i) applies, but for the moment we need the factor c_0^2 because of the weaker conclusion of (iii).

(v) This follows from parts (i) and (iii) and Lemma 11.5. □

Note that $D(X)$ vanishes on U^* and is constant on $V^* \setminus U^* = A$. So the value $D(x_0)$ is not in fact dependent on x_0 and equally, not dependent on any particular choice of $e_1, \ldots, e_{2n}$. In fact

$$D(x_0) = \prod_A x$$

is the special additional invariant η of $Sp(V)$ introduced in Lemma 8.4. Lemma 11.5 shows that

$$D(x_0) = P^+(0)P^-(0),$$

and so $D(x_0)$ also has its square in the subring

$$\mathbb{F}_2[\xi_0, \xi_1, \ldots, \xi_{2n-1}, c_{2n-1}, \ldots, c_n].$$

We conclude this section with a remark about Q^- which is needed later. Let W be a maximal b-isotropic subspace of U. Such a subspace of U has dimension n. Any quadratic form polarizing to b restricts to a linear functional on W because its polarization vanishes on W. The quadratic forms of $-$type restrict to non-zero linear functionals on W and every such linear functional on W arises in this way. Since every automorphism of W arises as the restriction of some symplectic automorphism of V it follows that the restriction of $Q^-(t^2)$ to W is a power of the Dickson polynomial for W. On grounds of degree we therefore have

LEMMA 11.7. *The image of $Q^-(t^2)$ in $S(W^*)[t]$ is*

$$\left(\prod_{0 \neq x \in W^*} (t + x) \right)^{2^n}.$$

12. 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

$$\mathbb{F}_2[X, \xi_1, \xi_2, \xi_3, \ldots] \to S[X]$$

defined by $X \mapsto X$ and $\xi_i \mapsto \xi_i$.

LEMMA 12.1. (i) $\Omega_{2n}(X) = \sum_{i=0}^{2n} (\Lambda_{2n,i})^2 X^{2^i} + \delta$ *where* $\delta \in \mathbb{F}_2[\xi_1, \xi_2, \ldots, \xi_{2n}]$.

(ii) *In the ring S we have $\Omega_{2n}(X) = c_0^2 Q(X)$.*

(iii) $\Omega_{2n}(X) = c_0^2 Q^-(X)Q^+(X)$, *and c_0, $Q^-(X)$ and $Q^+(X)$ are irreducible elements of the ring $S(U^*)^{Sp[U]}[X]$.*

(iv) $c_0 Q^-(X)$ *and* $c_0 Q^+(X)$ *both belong to* $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$.

Proof. (i) Looking at the standard expansion of the determinant A_{2n} we see first that any term involving a product of two or more of the diagonal entries will have a coefficient divisible by 4. So these make zero contribution to Ω_{2n}. For $0 \leq i \leq 2^{2n}$, we see that the coefficient of X^{2^i} in Ω_{2n} is precisely the determinant of the matrix $A_{2n,i}$

obtained by omitting the ith row and column (counting from 0 to $2n$) from $C^T B_0 C$. This determinant is equal to $(\Lambda_{2n,i})^2$ as noted in the proof of Lemma 10.2(i).

(ii) Recall Definition 11.2 that $Q(X) = \prod_{q\in B}(X+q)$ where $B = \{\xi_0 + x_0^2 + x^2;\ x \in U^*\}$. Using Dickson's Theorem (see Definition 5.6), we know that the polynomial $D'(X) := \sum_{i=0}^{2n} c_i^2 X^{2^i}$ has zero set precisely $\{x^2;\ x \in U^*\}$. (Note that $D'(x^2) = D(x)^2$.) Thus

$$Q(X) = D'\big(X + \xi_0 + x_0^2\big) = D'(X) + D'\big(\xi_0 + x_0^2\big).$$

We claim that $\Omega_{2n} = c_0^2 Q(X)$. First, it follows from Lemma 10.2(i) that $c_0^2 D'(X) = \sum_{i=0}^{2n} (\Lambda_{2n,i})^2 X^{2^i}$ and by part (i), this coincides with the part of $\Omega_{2n}(X)$ which involves X. Therefore

$$c_0^2 Q(X) + \Omega_{2n}(X)$$

does not involve X and to prove that it is zero it suffices to prove that

$$\Omega_{2n}\big(\xi_0 + x_0^2\big) = 0.$$

To this end we need to work over $\mathbb{Z}$ rather than $\mathbb{F}_2$ and we shall temporarily work with two abstract polynomial 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

$$\alpha(\xi_i) = \sum_{\ell=1}^{n} \big(x_{2\ell-1}^{2^i} x_{2\ell} + x_{2\ell-1} x_{2\ell}^{2^i}\big),$$

and

$$\alpha(X) = \sum_{\ell=1}^{n} x_{2\ell-1} x_{2\ell}.$$

Consider the matrices C and $B_0 C^T$ over $\mathbb{Z}$, and insert respectively a row and a column of zeros to make the matrices square. Then clearly they have determinant equal to zero, and further we have the matrix equation:

$$\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_{2n} & 0 \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_{2n}^2 & 0 \\ x_1^4 & x_2^4 & x_3^4 & \dots & x_{2n}^4 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{2^{2n}} & x_2^{2^{2n}} & x_3^{2^{2n}} & \dots & x_{2n}^{2^{2n}} & 0 \end{pmatrix} \begin{pmatrix} x_2 & x_2^2 & x_2^4 & \dots & x_2^{2^{2n}} \\ x_1 & x_1^2 & x_1^4 & \dots & x_1^{2^{2n}} \\ x_4 & x_4^2 & x_4^8 & \dots & x_4^{2^{2n}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{2n-1} & x_{2n-1}^2 & x_{2n-1}^4 & \dots & x_{2n-1}^{2^{2n}} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

$$= \alpha \begin{pmatrix} 2X & \xi_1 & \xi_2 & \xi_3 & \dots & \xi_{2n} \\ \xi_1 & 2X^2 & \xi_1^2 & \xi_2^2 & \dots & \xi_{2n-1}^2 \\ \xi_2 & \xi_1^2 & 2X^4 & \xi_1^4 & \dots & \xi_{2n-2}^4 \\ \xi_3 & \xi_2^2 & \xi_1^4 & 2X^8 & \dots & \xi_{2n-3}^8 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{2n} & \xi_{2n-1}^2 & \xi_{2n-2}^4 & \xi_{2n-3}^8 & \dots & 2X^{2^{2n}} \end{pmatrix}.$$

On taking determinants we find that $\alpha(H_{2n}) = 0$ and hence $\alpha(\frac{1}{2}H_{2n}) = 0$. (Recall from the remarks preceding Definition 9.1 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 $\mathbb{Z} \to \mathbb{F}_2$ is $\Omega(\xi_0 + x_0^2)$ and hence $\Omega(\xi_0 + x_0^2) = 0$ as required.

(iii) By part (ii), $\Omega_{2n} = c_0^2 Q(X) = c_0^2 Q^-(X)Q^+(X)$. The Dickson element c_0 and the quadratic Chern polynomials $Q^\pm(X)$ are irreducible as the symplectic group transitively permutes their factors.

(iv) Lemma 11.6(ii) deals with the case of $c_0 Q^-(X)$. Part (iv) of that Lemma says that $c_0^2 Q^+(X)$ belongs to our target ring. Thus we have

$$\begin{aligned} c_0^3 Q^+(X)Q^-(X) &= c_0^2 Q^+(X) \cdot c_0 Q^-(X) \\ &= c_0 \cdot \Omega_{2n}(X), \end{aligned}$$

and this 2-way factorization happens in the polynomial ring $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$. In this ring, c_0 is prime. Hence either c_0 divides $c_0 Q^-(X)$ or c_0 divides $c_0^2 Q^+(X)$ in $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$.

Suppose that $c_0 \mid c_0 Q^-(X)$, so that $Q^-(X) \in \mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$. By Lemma 11.5 and Lemma 11.7, the restriction of $Q^-(X)$ to a maximal isotropic subspace W of V involves Dickson invariants for W. As each ξ_i restricts to zero on W, it follows that $Q^-(X)$ involves Dickson invariants of U. This contradicts the assumption, so it must be the case that $c_0 \mid c_0^2 Q^+(X)$ in $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$, and $c_0 Q^+(X) \in \mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$ as claimed. □

Definition 12.2. Motivated by the previous Lemma, we define polynomials $\Omega_{2n}^+(X)$ and $\Omega_{2n}^-(X)$ in $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$ by

$$\Omega_{2n}^+(X) := c_0 Q^+(X), \quad \Omega_{2n}^-(X) := c_0 Q^-(X).$$

Part (iii) of the Lemma says that $\Omega_{2n}(X) = \Omega_{2n}^+(X)\Omega_{2n}^-(X)$.

Lemma 12.3. *These polynomials have the following properties.*

(i) $\Omega_{2n}^-(X)$ *and* $\Omega_{2n}^+(X)$ *are irreducible in the polynomial ring* $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$.

(ii) $\Omega_{2n}^\pm(X)$ *are both linear in* ξ_{2n} *with coefficients* $(\Omega_{2n-2}^\pm(X))^2$.

Proof. (i) Lemma 12.1 part (iv) says that $\Omega_{2n}^\pm(X) \in \mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$, and part (iii) that c_0, $Q^+(X)$ and $Q^-(X)$ are irreducible elements of the ring

$$S(U^*)^{Sp(U)}[X] = \mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}, c_{2n-1}, \ldots, c_n].$$

Thus if $\Omega_{2n}^\pm(X)$ were reducible in the smaller ring $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$ it would factorize as $c_0 \cdot Q^\pm(X)$. By the argument in Lemma 12.1 part (iv) we know however that $Q^\pm(X)$ is not in $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$, so $\Omega_{2n}^\pm(X)$ is irreducible in that ring as claimed.

(ii) View $\Omega_{2n}(X)$ as a polynomial in ξ_{2n} with coefficients in $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n-1}]$. From the Definition 9.1 of $\Omega_{2n}(X)$ via the determinant H_{2n} we see that $\Omega_{2n}(X)$ is quadratic in ξ_{2n} and

$$\Omega_{2n}(X) = \xi_{2n}^2 \Omega_{2n-2}(X)^2 + \xi_{2n}\text{-linear terms.}$$

By Lemma 12.1 part (iii), the quadratic term is $\xi_{2n}^2(\Omega_{2n-2}^-(X))^2(\Omega_{2n-2}^+(X))^2$. By part (i), each of ξ_{2n}, $\Omega_{2n-2}^+(X)$ and $\Omega_{2n-2}^-(X)$ is irreducible in the polynomial ring $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n}]$. Further, $\Omega_{2n}(X) = \Omega_{2n}^+(X)\Omega_{2n}^-(X)$, and a degree argument now delivers the result. □

LEMMA 12.4. (i) *If q is any quadratic form of $-$type then*

$$\begin{aligned}\Omega^-_{2n}(q) &= 0\\ \Omega^+_{2n}(q) &= c_0 \prod_{q+x^2 \text{ has } +type} x^2\\ \Omega^-_{2n-2}(q) &= \prod_{x\neq 0 \ \&\ q+x^2 \text{ has } -type} x\end{aligned}$$

(ii) *If q is any quadratic form of $+$type then*

$$\begin{aligned}\Omega^-_{2n}(q) &= c_0 \prod_{q+x^2 \text{ has } -type} x^2\\ \Omega^+_{2n}(q) &= 0\\ \Omega^+_{2n-2}(q) &= \prod_{x\neq 0 \ \&\ q+x^2 \text{ has } +type} x\end{aligned}$$

(iii) *The following is an identity:*

$$(\Omega^+_{2n-2}(X))^2\Omega^-_{2n}(X) + (\Omega^-_{2n-2}(X))^2\Omega^+_{2n}(X) = \Lambda^3_{2n}.$$

Proof. (i) Fix a q of $-$type. By definition $\Omega^-_{2n}(X) = c_0 \prod_{r\in B^-}(X+r)$ and we immediately have the first equation $\Omega^-_{2n}(q) = 0$. For the second equation, notice that for any form r of $+$type, $q + r = x^2$ for some $x \in U^*$ with $r = q + x^2$, so we have

$$\Omega^+_{2n}(q) = c_0 \prod_{r\in B^\pm}(q+r) = c_0 \prod_{q+x^2\in B^+}(x^2).$$

Turning to the third equation, let x be a non-zero element of U^* such that $q + x^2$ has $-$type. Let $W = \operatorname{Ker} x$ be the codimension one subspace of U on which x vanishes. As in the discussion in Secion 4, following the statement of Witt's Theorem, we know that the restriction of q to W is either non-singular or it is of $-$type. Since $q + x^2$ has $-$type, Lemma 4.3 states that q restricts to a $-$type form on W. Therefore by applying the first equation we have here to the lower dimensional space W, we deduce that $\Omega^-_{2n-2}(X)$ vanishes on $q|W$, and therefore

$$\Omega^-_{2n}(q)$$

is divisible by x. This is true for all $x \neq 0$ such that $q + x^2$ has $-$type and therefore $\Omega^-_{2n}(q)$ is divisible by the product of all such x. The result now follows by a degree argument.

(ii) Similar to part (i). At this stage, the $+$type case runs entirely in parallel to the $-$type case.

(iii) The left side of the equation is a polynomial with degree in X at most equal to

$$\begin{aligned}2\deg(\Omega^+_{2n-2}(X)) + \deg(\Omega^-_{2n}(X)) &= 2(2^{2n-3} - 2^{n-2}) + (2^{2n-1} + 2^{n-1})\\ &= (2^{2n-1} + 2^{2n-2})\\ (\,&= 2\deg(\Omega^-_{2n-2}(X)) + \deg(\Omega^+_{2n}(X))\,)\end{aligned}$$

which is less than 2^{2n}, the number of quadratic forms of + or − type. Thus if the equality holds when evaluated on every such form, it is an identity.

Now let q be a form, say of +type. By parts (i) and (ii), the second summand of the left hand side is zero, and the first is equal to

$$\begin{aligned}(\Omega^+_{2n-2}(q))^2\Omega^-_{2n}(q) &= \left(\prod_{x\neq 0 \ \&\ q+x^2 \text{ has } +\text{type}} x\right)^2 \left(c_0 \prod_{q+x^2 \text{ has } -\text{type}} x^2\right)\\ &= c_0 \prod_{x\in U^*,\ x\neq 0} x^2\\ &= c_0^3\end{aligned}$$

which is equal to Λ^3_{2n} by Lemma 10.2 (i).

The calculation is similar if q is a form of −type, so as noted above we are done. □

This has important consequences for the Chern polynomials $P^{\pm}(t)$.

COROLLARY 12.5. *The coefficient of t in $P^{\pm}(t)$ is $\Omega^{\pm}_{2n-2}(\xi_0)$.*

Proof. We deal with the −case, the proof in the +case being obtained simply by replacing + by − throughout the argument. Let s be the coefficient of t in $P^-(t)$. Let $x_- \in A^-$ be any vector of −type (i.e. $\xi_0 + x_-^2$ has −type). On restricting to the subspace $\operatorname{Ker} x_-$ we have

$$P^-(t)|_{\operatorname{Ker} x_-} = t \cdot \prod_{x'}(t + x')$$

where x' runs through the non-zero vectors in $\operatorname{Ker} x_-$ such that $\xi_0 + x_-^2 + x'^2$ has −type. Equating coefficients of t we see that

$$s|_{\operatorname{Ker} x_-} = \prod_{x'} x' = \Omega^-_{2n-2}(\xi_0 + x_-^2),$$

by Lemma 12.4(i). Hence $s \equiv \Omega^-_{2n-2}(\xi_0)$ modulo x_-. This is true for all $x_- \in A^-$ and hence $s \equiv \Omega^-_{2n-2}(\xi_0)$ modulo $\prod x_- = P^-(0)$. Now $P^-(0)$ has degree greater than s, and so in fact we have

$$s = \Omega^-_{2n-2}(\xi_0)$$

as claimed. □

LEMMA 12.6. *Viewing $\Omega^{\pm}_{2n}(X)$ as a polynomial in X:*

(i) $\Omega_{2n}(X) = (\Lambda_{2n})^2 X^{2^{2n}} +$ *terms involving lower powers of* X.
(ii) $\Omega^+_{2n}(X) = \Lambda_{2n} X^{2^{2n-1}+2^{n-1}} +$ *terms involving lower powers of* X.
(iii) $\Omega^-_{2n}(X) = \Lambda_{2n} X^{2^{2n-1}-2^{n-1}} +$ *terms involving lower powers of* X.

The proof of this is trivially a consequence of the Definition 12.2.

LEMMA 12.7. (i) $\Omega^+_{2n-2}(t^2+\xi_0)P^-(t) + \Omega^-_{2n-2}(t^2+\xi_0)P^+(t) = \Lambda_{2n}$,
(ii) $\Lambda_{2n}P^-(t) = \Omega^+_{2n-2}(t^2+\xi_0)Q^-(t^2+\xi_0) + \Omega^-_{2n-2}(t^2+\xi_0)\,(D(t) + D(x_0))$,
(iii) $\Lambda_{2n}P^+(t) = \Omega^-_{2n-2}(t^2+\xi_0)Q^+(t^2+\xi_0) + \Omega^+_{2n-2}(t^2+\xi_0)\,(D(t) + D(x_0))$.

Proof. The first equation follows immediately from Lemma 12.4 (iii), putting $X = t^2 + \xi_0$, dividing by Λ_{2n} and taking the square root. The second follows from the first through multiplying by $P^-(t)$ and using the third equality of Lemma 11.5. □

We conclude this section with statements of our calculations of the $\Omega^{\pm}_{2n}$ for small values of n.

EXAMPLE 12.8. For $n = 1$ we have

$$\begin{aligned}\Omega_2(X) &= \xi_1^2X^4 + \xi_2^2X^2 + \xi_1^4X + \xi_1^3\xi_2\\ \Omega_2^+(X) &= \xi_1X^3 + \xi_2X^2 + \xi_1^3\\ \Omega_2^-(X) &= \xi_1X + \xi_2\end{aligned}$$

For $n = 2$,

$$\begin{aligned}\Omega_4(X) = {} & \Lambda_4^2X^{16} + \Lambda_{4,3}^2X^8 + \Lambda_{4,2}^2X^4 + \Lambda_{4,1}^2X^2 + \Lambda_4^4X\\ & + \big(\xi_1^4\Lambda_{4,3} + \big(\xi_2^4 + \xi_2\xi_1^5\big)\Lambda_4\big)(\Lambda_{4,2} + \xi_1\xi_3\Lambda_4)\\ \Omega_4^+(X) = {} & \Lambda_4X^{10} + \xi_1^2\Lambda_4X^7 + (\Lambda_{4,3} + \xi_1\xi_2\Lambda_4)X^6 + \xi_2^2\Lambda_4X^5\\ & + \big(\Lambda_{4,2} + \big(\xi_1\xi_3 + \xi_1^4\big)\Lambda_4\big)X^4 + \xi_2^2\xi_1^2\Lambda_4X^2 + \xi_1^6\Lambda_4X\\ & + \xi_1^4\Lambda_{4,3} + \big(\xi_2^4 + \xi_2\xi_1^5\big)\Lambda_4\\ \Omega_4^-(X) = {} & \Lambda_4X^6 + \xi_1^2\Lambda_4X^3 + (\Lambda_{4,3} + \xi_1\xi_2\Lambda_4)X^2 + \xi_2^2\Lambda_4X + (\Lambda_{4,2} + \xi_1\xi_3\Lambda_4)\end{aligned}$$

For $n = 0$ it makes sense to define $\Omega_0^+(X) := X$ and $\Omega_0^-(X) := 1$.

When $n = 3$ the calculation is formidable. The factors $\Omega_6^-(X)$ and $\Omega_6^+(X)$ have degrees 119 and 135 respectively. The calculation was carried out directly from our definition of $\Omega_6(X)$ by Allan Steel using the Magma computer algebra package. His results are available on the first author's web site, [**14**].

13. The recursive calculation of $\Omega^-(X)$ and $\Omega^+(X)$. Here we begin with two results which enormously improve our understanding of $\Omega^{\pm}(X)$. Their proofs rely on a line of reasoning first used by Carlisle and Kropholler in dealing with the symplectic case and which we briefly review. Consider the inclusion of rings

$$\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}] \to S = \mathbb{F}_2[x_1, \ldots, x_{2n}]$$

We know that this is an inclusion by Lemma 8.5. We also know that this inclusion carries Λ_{2n} to the Dickson invariant c_0 as noted in the preamble to Section 10. If we take any non-zero element x of V^*, that is, a non-zero linear combination of the x_i then the composite

$$\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}] \to S \to S/xS$$

is not an inclusion because clearly, under the second map, c_0 is carried to zero. Therefore Λ_{2n} lies in the kernel I of this composite. Note, crucially, Λ_{2n} does not involve ξ_{2n}.

Now consider the restriction of this composite to the ring in which ξ_{2n} is omitted:

$$\mathbb{F}_2[\xi_1, \ldots, \xi_{2n-1}] \to S/xS.$$

Again, by Lemma 8.5 (this time applied to the $2n-2$ dimensional case) we know that the images of $\xi_1, \ldots, \xi_{2n-2}$ are algebraically independent. Moreover, Λ_{2n} remains present as an element of the kernel. Since Λ_{2n} is irreducible by Lemma 10.2(ii), it follows on simple Krull dimension grounds that the kernel of our restricted composite is exactly the principal ideal on Λ_{2n}.

In conclusion: if an element of $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$ does not involve ξ_{2n} but its image in S is divisible by c_0 then such an element lies in the kernel of the map to S/xS for any choice of x as above; therefore it is an element of the restricted kernel and hence it is intrinsically a multiple of Λ_{2n} within the ring $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$.

By contrast, notice that we cannot draw the same conclusion about such an element when it does involve ξ_{2n}. Indeed the conclusion fails in many relevant cases: for example, we know that $c_0 c_i$ is always expressible within $\mathbb{F}_2[\xi_1, \ldots, \xi_{2n}]$ and is patently a multiple of c_0 in the ambient ring S. But for $1 \leq i \leq 2n-1$ these elements are never multiples of Λ_{2n} intrinsically.

In the first part of the following Proposition, and again in its companion Proposition 13.2, we need the above conclusion. We arrange the inductive hypothesis so that, at a key point, the polynomial we are dealing with does not involve ξ_{2n}.

PROPOSITION 13.1. *In the abstract polynomial ring* $\mathbb{F}_2[X, \xi_1, \xi_2, \ldots]$ *there is a sequence of polynomials* $\alpha_n^+(X)$ *for* $n \geq 0$ *with the following properties:*

(i) *For each* $n \geq 0$, $\alpha_n^+(X)$ *belongs to* $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n-1}]$ *and*

$$\Omega_{2n}^+(X) = \sum_{\ell=0}^{n} \Lambda_{2n,n+\ell}(\alpha_\ell^+(X))^{2^{n-\ell}}.$$

(ii) $\alpha_n^+(X)$ *is monic in* X *with* X*-degree* $2^{2n-1} + 2^{n-1}$.

(iii)

$$\begin{aligned}
\alpha_0^+(X) &= X \\
\alpha_1^+(X) &= X^3 + \xi_1^2 \\
\alpha_2^+(X) &= X^{10} + \xi_1^2 X^7 + \xi_2\xi_1 X^6 + \xi_2^2 X^5 \\
&\quad + \left(\xi_3\xi_1 + \xi_1^4\right) X^4 + \xi_2^2\xi_1^2 X^2 + \xi_1^6 X + \xi_2^4 + \xi_2\xi_1^5.
\end{aligned}$$

(iv) $\alpha_n^+(X) \equiv \xi_n^{2^n}$ *modulo* $X, \xi_1, \ldots, \xi_{n-1}$.

(v) *For* $n \geq 1$, *the summand of* $\alpha_n^+(X)$ *comprising all those terms of odd degree in* X *is equal to* $(\Omega_{2n-2}^+(X))^2 X$.

Proof. (i) We construct the $\alpha_n^+(X)$ inductively. Notice first that $\Lambda_{2,1} = \xi_2$, $\Lambda_{2,2} = \Lambda_2 = \xi_1$, and therefore

$$\Omega_2^+(X) = \xi_1 X^3 + \xi_2 X^2 + \xi_1^3 = \Lambda_{2,1}(\alpha_0^+(X))^2 + \Lambda_2 \alpha_1^+(X)$$

confirming our formula when $n = 1$. We could be a little more economical by observing that the formula is also consistent with the case $n = 0$ given the definitions $\Omega_0^+(X) = X$ and $\Lambda_0 = 1$. Now suppose that $n \geq 2$ and that the $\alpha_j^+(X)$ have been chosen for $j < n$ so that

$$\Omega_{2n-2}^+(X) = \sum_{\ell=0}^{n-1} \Lambda_{2n,n+\ell}(\alpha_\ell^+(X))^{2^{n-\ell}}.$$

Then the coefficient of ξ_{2n} in $f(X) := \Omega^+_{2n}(X) - \sum_{\ell=0}^{n-1} \Lambda_{2n,n+\ell}(\alpha^+_\ell(X))^{2^{n-\ell}}$ is

$$(\Omega^+_{2n-2}(X))^2 - \sum_{\ell=0}^{n-1} (\Lambda_{2n-2,n+\ell-1})^2 (\alpha^+_\ell(X))^{2^{n-\ell}}$$

which is zero by induction. In other words, $f(X)$ does not involve ξ_{2n} and the opening remarks of this section can be applied to the coefficient of each power of X. We see that $f(X)$ is a polynomial in $X, \xi_1, \ldots, \xi_{2n-1}$ and since the coefficients of $f(X)$ as a polynomial in X are divisible by $c_0 = \Lambda_{2n}$ when we pass to their images in the ambient ring S it follows from the conclusion to the preamble, that $f(X)$ is also divisible by Λ_{2n} in the ring $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n-1}]$. Therefore we can (and must) set $\alpha^+_n(X) := f(X)/\Lambda_{2n}$.

(ii) This follows from Lemma 12.6. Working by induction on n we may suppose that $\alpha^+_\ell(X)$ is monic of X-degree $2^{2\ell-1} + 2^{\ell-1}$ for $\ell < n$. Lemma 12.6 says that $\Omega^+_{2n}(X)$ has X-degree $2^{2n-1} + 2^{n-1}$ which is greater than any of the contributions coming from $(\alpha^+_\ell(X))^{2^{n-\ell}}$ for $\ell < n$ in our new formula. Therefore only the term involving $\alpha^+_n(X)$ contributes to the highest power of X and Lemma 12.6 verifies our assertion that $\alpha^+_n(X)$ is monic.

(iii) This can be checked by direct calculation.

(iv) The total degree of $\alpha^+_n(X)$ of is $2^{2n} + 2^n$ because X has degree 2. Modulo $X, \xi_1, \ldots, \xi_{n-1}$, only monomials in $\xi_n, \ldots, \xi_{2n-1}$ can contribute. For such a monomial $\xi_n^{a_n} \cdots \xi_{2n-1}^{a_{2n-1}}$ to exist we need natural numbers $a_n, \ldots, a_{2n-1}$ such that

$$a_n(2^n + 1) + \cdots + a_{2n-1}(2^{2n-1} + 1) = 2^{2n} + 2^n.$$

Hence

$$a_n + \cdots + a_{2n-1} \equiv 0 \text{ modulo } 2^n.$$

Moreover we can also see that $a_j \leq 2^{n-j}$ for each j and therefore

$$a_n + \cdots + a_{2n-1} \leq 2^n + 2^{n-1} + \cdots + 2 < 2^{n+1}.$$

If the a_i are not all zero then the displayed information above implies that

$$a_n + \cdots + a_{2n-1} = 2^n,$$

and therefore

$$\begin{aligned} 2^n(2^n + 1) &= (a_n + \cdots + a_{2n-1})(2^n + 1) \\ &\leq a_n(2^n + 1) + \cdots + a_{2n-1}(2^{2n-1} + 1) \\ &= 2^{2n} + 2^n. \end{aligned}$$

Thus the inequality above must be equality. Hence $a_i = 0$ for $i > n$ and it follows that $a_n = 2^n$ and $\xi_n^{a_n} \cdots \xi_{2n-1}^{a_{2n-1}} = \xi_n^{2^n}$. From this we can conclude that $\alpha^+_n(X) \equiv 0$ or $\xi_n^{2^n}$ modulo $X, \xi_1, \ldots, \xi_{n-1}$. In particular, it follows that $\alpha^+_\ell(X) \equiv 0$ modulo $X, \xi_1, \ldots, \xi_{n-1}$ whenever $\ell < n - 1$, and so the recursive formula in (i) gives

$$\Omega^+_{2n}(0) \equiv \Lambda_{2n}\alpha^+_n(X) \qquad \text{mod } X, \xi_1, \ldots, \xi_{n-1}.$$

It can be seen directly from its definition that $\Omega_{2n}(X)$ involves the monomial $\xi_{n+1}^{2^n-1}\xi_n^{2^{n+1}-1}$ and therefore $\Omega_{2n}(X) \not\equiv 0$, $\Omega_{2n}^+(X) \not\equiv 0$, and $\alpha_n^+(X) \not\equiv 0$. Thus $\alpha_n^+(X) \equiv \xi_n^{2^n}$ modulo $X, \xi_1, \ldots, \xi_{n-1}$ as claimed.

(v) From the identity we have proved in (i), we see that the terms of odd degree within $\Omega_{2n}^+(X)$ are exactly the terms of odd degree within $\Lambda_{2n}\alpha_n^+(X)$. Since $\Omega_{2n}^+(X) = \Lambda_{2n}Q^+(X)$ it follows that $\alpha_n^+(X)$ and $Q^+(X)$ have the same odd degree part.

Let $X \cdot g(X)$ denote the odd degree component of $Q^+(X)$. It now suffices to prove that $g(X) = (\Omega_{2n-2}^+(X))^2$. This follows from Corollary 12.5, together with the first identity of Lemma 11.5: $(P^+(t))^2 = Q^+(t^2 + \xi_0)$. Corollary 12.5 says that $(\Omega_{2n-2}^+(\xi_0))^2$ is equal to the coefficient of t^2 in $(P^+(t))^2$. Through Lemma 11.5, this in turn is equal to the coefficient of t^2 in $Q^+(t^2 + \xi_0)$ and since it is precisely the odd powers of t^2 which contribute to this, the coefficient is $g(\xi_0)$. Thus $(\Omega_{2n-2}^+(\xi_0))^2 = g(\xi_0)$ and, in view of the generic nature of ξ_0, the result follows. □

PROPOSITION 13.2. *In the abstract polynomial ring $\mathbb{F}_2[X, \xi_1, \xi_2, \ldots]$ there is a sequence of polynomials $\alpha_n^-(X)$ for $n \geq 0$ with the following properties:*

(i) *For each $n \geq 0$, $\alpha_n^-(X)$ belongs to $\mathbb{F}_2[X, \xi_1, \ldots, \xi_{2n-1}]$ and*

$$\Omega_{2n}^-(X) = \sum_{\ell=0}^{n} \Lambda_{2n,n+\ell}(\alpha_\ell^-(X))^{2^{n-\ell}}.$$

(ii) *$\alpha_n^-(X)$ is monic in X with X-degree $2^{2n-1} - 2^{n-1}$.*

(iii)

$$\begin{aligned}\alpha_0^-(X) &= 1\\ \alpha_1^-(X) &= X\\ \alpha_2^-(X) &= X^6 + \xi_1^2X^3 + \xi_2\xi_1X^2 + \xi_2^2X + \xi_3\xi_1.\end{aligned}$$

(iv) *For $n \geq 1$, $\alpha_n^-(X) \equiv 0$ modulo $X, \xi_1, \ldots, \xi_{n-1}$.*

(v) *For $n \geq 1$, the part of α_n^- which has odd degree in X is equal to $(\Omega_{2n-2}^-(X))^2X$.*

Proof. The proof proceeds in just the same way as for the α^+. We leave the details to the reader. Just one remark: the degree argument for part (iv) goes along rather more swiftly in this case but notice that while the conclusion is stronger for $n \geq 1$ the case $n = 0$ is a significant exception to the rule. □

COROLLARY 13.3. *For each $n \geq 1$, we have that $\Omega_{2n}^+(X) \equiv \xi_n^{2^{n+1}-1}$ and $\Omega_{2n}^-(X) \equiv \Lambda_{2n,n}$ modulo $X, \xi_1, \ldots, \xi_{n-1}$. Also, $\Omega_{2n}^-(X) \equiv \xi_{n+1}^{2^n-1}$ modulo $\xi_1, \ldots, \xi_n$.*

Proof. Using the above Propositions we find that

$$\Omega_{2n}^+(X) \equiv \Lambda_{2n}\alpha_n^+(X) \equiv \Lambda_{2n}\xi_n^{2^n}$$

and

$$\Omega_{2n}^-(X) \equiv \Lambda_{2n,n}\alpha_0^-(X) = \Lambda_{2n,n}$$

modulo $X, \xi_1, \ldots, \xi_{n-1}$. This demonstrates the result for Ω^-. It is also straightforward to see from its definition that $\Lambda_{2n} \equiv \xi_n^{2^n-1}$ and the result for Ω^+ now follows as well. Working modulo $\xi_1, \ldots, \xi_n$ for the last part, it is straightforward to use degree

arguments to see that $\Lambda_{2n,n+j} \equiv 0$ for $j \geq 1$ and by direct calculation that $\Lambda_{2n,n} \equiv \xi_{n+1}^{2^n-1}$. These facts yield the third stated equivalence. □

COROLLARY 13.4. *Let $j \geq 0$ be a natural number and let P_j be the coefficient of degree j in $P^-(t)$, (i.e. P_j is the coefficient of $t^{2^{2n-1}-2^{n-1}-j}$). Let P'_j be the coefficient of degree $j-1$ in $\Omega^-_{2n-2}(t^2+\xi_0)$, (i.e. P'_j is the coefficient of $t^{2^{2n-1}-2^{n-1}-j}$). Then*

$$Sq^j\Omega^-_{2n-2}(\xi_0) = \Omega^-_{2n-2}(\xi_0)P_j + P'_jP^-(0).$$

Proof. If $j = 0$ then $P_0 = 1$ and we define $P'_0 := 0$. Assume that $j \geq 1$. Using Lemma 12.5 together with Lemma 3.2 we have

$$Sq^j\Omega^-_{2n-2}(\xi_0) \equiv \Omega^-_{2n-2}(\xi_0)P_j$$

modulo x_- for all $x_- \in A^-$. Hence $P^-(0) = \prod x_-$ divides $Sq^j\Omega^-_{2n-2}(\xi_0) + \Omega^-_{2n-2}(\xi_0)P_j$ and there is an invariant P'_j such that

$$Sq^j\Omega^-_{2n-2}(\xi_0) = \Omega^-_{2n-2}(\xi_0)P_j + P'_jP^-(0).$$

Since $\Omega^-_{2n-2}(\xi_0)$ involves only $\xi_0, \ldots, \xi_{2n-2}$, when we apply the Steenrod operation Sq^j the result is a polynomial in $\xi_0, \ldots, \xi_{2n-1}$. Therefore if we square the above displayed equation and multiply by Λ_{2n} the left hand side does not involve ξ_{2n} whilst the right hand side simplifies to the expression

$$\begin{aligned}&(\Omega^-_{2n-2}(\xi_0))^2\Lambda_{2n}(P_j)^2 + (P'_j)^2\Lambda_{2n}(P^-(0))^2\\ &\quad= (\Omega^-_{2n-2}(\xi_0))^2\left[\sum_{\ell=0}^{n}\Lambda_{2n,n+\ell}(\alpha^-_\ell(t^2+\xi_0))^{2^{n-\ell}}\right]_{[2j+2^{2n}-1]} + (P'_j)^2\Omega^-_{2n}(\xi_0),\end{aligned}$$

where the notation $[\ ]_{[2j+2^{2n}-1]}$ means "pick out the coefficient of degree $2j + 2^{2n} - 1$" from the polynomial in t. Thus, equating coefficients of ξ_{2n} we have

$$0 = (\Omega^-_{2n-2}(\xi_0)[\Omega^-_{2n-2}(t^2+\xi_0)]_{[j-1]} + P'_j\Omega^-_{2n-2}(\xi_0))^2$$

Taking square roots and dividing by $\Omega^-_{2n-2}(\xi_0)$ we conclude that

$$P'_j = [\Omega^-_{2n-2}(t^2+\xi_0)]_{[j-1]}$$

as required. □

COROLLARY 13.5. $(\Omega^-_{2n-4}(\xi_0))^2\xi_{2n-1} + \Omega^-_{2n-2}(\xi_0)d_{2n-1} + \Lambda_{2n-2}d_n$ *belongs to the subring generated by* $\xi_0, \ldots, \xi_{2n-2}$

Proof. Take $j := 2^{2n-2}$ in Corollary 13.4. Since

$$\Omega^-_{2n-2}(X) = \xi_{2n-2}(\Omega^-_{2n-4}(X))^2 + \text{ terms in } X, \xi_1, \ldots, \xi_{2n-3}$$

it follows from Lemma 5.4 and its Corollary that

$$Sq^{2^{2n-2}}(\Omega^-_{2n-2}(X)) = \xi_{2n-1}(\Omega^-_{2n-4}(X))^2 + \text{ terms in } X, \xi_1, \ldots, \xi_{2n-2}.$$

Therefore by Corollary 13.4 we have

$$\xi_{2n-1}(\Omega^-_{2n-4}(X))^2 + \text{ terms in } X, \xi_1, \ldots, \xi_{2n-2} = \Omega^-_{2n-2}(\xi_0)P_{2^{2n-2}} + P'_{2^{2n-2}}d_n,$$

where $P'_{2^{2n-2}}$ is the coefficient of degree $2^{2n-2}-1$ in $\Omega^-_{2n-2}(t^2+\xi_0)$. Using Lemma 12.6 we can see that $P'_{2^{2n-2}} = \Lambda_{2n-2}$ and the desired conclusion follows. □

COROLLARY 13.6. *The coefficients of $\Omega^-_{2n-2}(\xi_0)P^-(t)$ lie in $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}, d_n]$. The $2n+1$ elements $\xi_0, \ldots, \xi_{2n-1}, d_n$ are algebraically independent in S and the $2n+2$ elements $\xi_0, \ldots, \xi_{2n-1}, d_n, d_{2n-1}$ satisfy a single relation in S which is linear in $\xi_{2n-1}, d_n, d_{2n-1}$.*

Proof. The first part is immediate from Corollary 13.4. Now we know that S is integral over the ring generated by the coefficients of $P^-(t)$ at least for $n \geq 2$. It follows that S is algebraic over $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}, d_n]$ and so on grounds of Krull dimension, $\xi_0, \ldots, \xi_{2n-1}, d_n$ must be algebraically independent. The last part now follows at once. The relation is as described in Corollary 13.5 □

COROLLARY 13.7. *Let R denote the subring $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-2}]$.*

(i) $\{s \in R;\ sd_{2n-1} \in \xi_{2n-1}R + d_nR\} = \Omega^-_{2n-2}(\xi_0)R$,
(ii) $\{s \in R;\ sd_n \in \xi_{2n-1}R + d_{2n-1}R\} = \Lambda_{2n-2}R$,
(iii) $\{s \in R;\ s\xi_{2n-1} \in d_{2n-1}R + d_nR\} = \Omega^-_{2n-4}(\xi_0)^2R$.

Proof. This follows in a manner similar to the proof of Lemma 10.3 using the fact that $\Omega^-_{2n-2}(\xi_0), \Lambda_{2n-2}, \Omega^-_{2n-4}(\xi_0)$ are distinct irreducible elements of $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-2}]$. □

We have the following consequence which is crucial in our calculations:

LEMMA 13.8. *There is a matrix $\mathbf{J}_n$ and column vector $\mathbf{F}_n$ so that*

$$\begin{pmatrix} c_n \\ \vdots \\ c_{2n-1} \end{pmatrix} = \mathbf{J}_n^{*2} \begin{pmatrix} d_n^2 \\ \vdots \\ d_{2n-1}^2 \end{pmatrix} + \mathbf{F}_n.$$

Here, $\mathbf{J}_n^{*2}$ denotes the matrix whose entries are the squares of the entries of the matrix $\mathbf{J}_n$. The matrix $\mathbf{J}_n$ is upper uni-triangular with entries in the subring generated by $\xi_0, \ldots, \xi_{2n-3}$ and $\mathbf{F}_n$ is a column of polynomials in $\xi_0, \ldots, \xi_{2n-2}$.

Proof. From the formula

$$(P^-(t))^2 = Q^-(t^2+\xi_0) = \sum_{\ell=0}^{n} c_{n+\ell}(\alpha^-_\ell(t^2+\xi_0))^{2^{n-\ell}}$$

we see that on equating appropriate powers of t,

$$d_j^2 = c_j + \text{ terms involving and linear in } c_{j+1}, \ldots, c_{2n-1}, c_{2n}.$$

Note that $c_{2n} = 1$. Moreover the coefficients of c_k here are all squares for $j+1 \leq k \leq 2n-1$. So there is an upper uni-triangular matrix $\mathbf{U}_n$ and a column $\mathbf{V}_n$ both having

polynomial entries in the ξ's such that

$$\begin{pmatrix} d_n^2 \\ \vdots \\ d_{2n-1}^2 \end{pmatrix} = \mathbf{U}_n^{*2} \begin{pmatrix} c_n \\ \vdots \\ c_{2n-1} \end{pmatrix} + \mathbf{V}_n.$$

We obtain the required form of result by setting $\mathbf{J}_n := \mathbf{U}_n^{-1}$ and then $\mathbf{F}_n := \mathbf{J}_n^{*2}\mathbf{V}_n$. □

COROLLARY 13.9. *The subring of S generated by $\xi_0, \ldots, \xi_{2n-1}$ together with $d_{2n-1}, \ldots, d_n$ contains all the coefficients of $P^-(t)$.*

Proof. Let P_j be the coefficient of $P^-(t)$ of degree j. The formula

$$P^-(t)^2 = \sum_{\ell=0}^{n} c_{n+\ell}(\alpha_\ell^-(t^2 + \xi_0))^{2^{n-\ell}}$$

shows that P_j^2 can be expressed as a linear combination of $c_n, \ldots, c_{2n-1}, c_{2n} = 1$ with coefficients in the subring $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$ and for $\ell < n$, the coefficient of $c_{n+\ell}$ in this expression is a square. From this, together with the Lemma above, we see that there is a linear combination

$$\lambda_{2n-1}d_{2n-1} + \cdots + \lambda_n d_n$$

with each λ_i belonging to $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$ such that

$$P_j^2 = (\lambda_{2n-1}d_{2n-1} + \cdots + \lambda_n d_n)^2 + \lambda$$

for some $\lambda \in \mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$. Clearly λ is a square in the ambient ring S and therefore it is a square in the subring $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$ by Lemma 10.4. So

$$P_j = \lambda_{2n-1}d_{2n-1} + \cdots + \lambda_n d_n + \sqrt{\lambda},$$

as required. □

COROLLARY 13.10. *The coefficients of $P^+(t)$ also belong to the subring specified by the corollary above.*

Proof. This can be proved in just the same way, using the formula

$$P^+(t)^2 = \sum_{\ell=0}^{n} c_{n+\ell}(\alpha_\ell^+(t^2 + \xi_0))^{2^{n-\ell}}.$$

□

14. The invariants of $O(V)$. Define T to be the subring of S generated by $\xi_0, \xi_1, \ldots, \xi_{2n-1}, d_{2n-1}, \ldots, d_n$. This section is devoted to proving that T is the ring of invariants of $O(V)$. If $n \geq 2$ then the set A^- of vectors in V^* of $-$type spans V^* and hence S is an integral and separable extension of the subring generated by the coefficients of $P^-(t)$. When $n = 0$ or 1, A^- does not span V^*, but in these cases the A^+ spans V^* and so at least we can say that S is integral and separable over the subring generated by the coefficients of $P^+(t)$. The Corollaries following Lemma 13.8 say that our chosen subring T contains the coefficients of both $P^-(t)$ and $P^+(t)$. Therefore

LEMMA 14.1. *S is integral and separable over T and the field of fractions $ff(T)$ of T is the fixed field $ff(S)^{O(V)}$.*

Proof. Only the remark about fields of fractions remains to be proved. We chose the generators of T to be invariant and so $ff(T) \subseteq ff(S)^{O(V)}$. Let G be the Galois group of the extension $ff(T) \subseteq ff(S)$. (The first part of this Lemma shows that the extension is Galois.) Then G fixes $\xi_0 \in ff(T)$ and so $G \subseteq O(V)$. Also $ff(T) \subseteq ff(S)^{O(V)}$ and so $G \supseteq O(V)$. Therefore $G = O(V)$ and $ff(T) = ff(S)^{O(V)}$. □

From this Lemma we see that the integral closure of T is the fixed ring for $O(V)$. In fact T *is* integrally closed. To prove this we consider a presentation of T as the quotient of a certain abstract polynomial ring T^*.

14.2. Working in T^*. Let T^* denote an abstract polynomial ring on $3n$ generators with weighted degrees in accordance with our chosen generators of T. We consider the surjection $T^* \to T$ defined by mapping the abstract generators to the corresponding generators of T. We shall call the generators of T^* by the obvious names:

$$\xi_0, \ldots, \xi_{2n-1}, d_{2n-1}, \ldots, d_n$$

in order to economize on notation. In practice this means keeping very clear the distinction between working in T^* and working in T. We shall identify a regular sequence $r_1, \ldots, r_{n-1}$ of elements of T^* which lie in the kernel of the map $T^* \to T$. We shall therefore find that there is an induced map

$$T^*/(r_1, \ldots, r_{n-1}) \to T.$$

The polynomials $\Omega^-_{2n-2}(\xi_0)$ and Λ_{2n-2} are polynomials in the ξ's which can be viewed as elements of T^* in the obvious way. We shall show that their images in $T^*/(r_1, \ldots, r_{n-1})$ satisfy the hypotheses of Proposition 1.1 and hence $T^*/(r_1, \ldots, r_{n-1})$ is a unique factorization domain and the map

$$T^*/(r_1, \ldots, r_{n-1}) \to T$$

is an isomorphism. Now clearly T is contained in the ring of invariants $S^{O(V)}$ and since it is integrally closed one only has to check the elementary Galois theory to conclude that

$$T = S^{O(V)}.$$

Note that T contains the Dickson invariants for U^* and the coefficients of both $P^-(t)$ and $P^+(t)$. Therefore T also contains $\eta = P^-(0)P^+(0)$ and so

$$S^{Sp(V)} \subset T.$$

This puts the Galois theory in place, and since any subgroup of $GL(V)$ which fixes the quadratic form ξ_0 is a subgroup of the orthogonal group we reach the desired conclusion.

We use the notation $\mathbf{M}^{*2}$ to indicate the matrix obtained from a matrix $\mathbf{M}$ by squaring all its entries. In case $\mathbf{M} = \mathbf{N}^{*2}$ for some $\mathbf{N}$ we also use the notation $\sqrt{\mathbf{M}}$ to denote the matrix $\mathbf{N}$ which is uniquely determined by $\mathbf{M}$ when it exists. We write $\mathbf{M}'$ for the matrix obtained from $\mathbf{M}$ by omitting the first row.

14.3. The subring of S generated by $\xi_0, \dots, \xi_{2n}$ together with $d_{2n-1}, \dots, d_n$. We begin by considering the subring of S generated by $\xi_0, \dots, \xi_{2n}, d_{2n-1}, \dots, d_n$. This makes a total of $3n+1$ generators. Recall (8.3): the fundamental relations for the symplectic invariants $S(U^*)^{Sp(U)}$

$$(\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n)\begin{pmatrix} c_n \\ \vdots \\ c_{2n-1}\end{pmatrix} = \begin{pmatrix} \xi_{2n} \\ \vdots \\ \xi_{n+1}^{2^{n-1}}\end{pmatrix} + \mathbf{L}_n\mathbf{E}_n$$

The following observations are significant:

LEMMA 14.4. (i) *The $(n-1)\times(n-1)$ matrix obtained by omitting the first row and last column of $\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n$ is $(\mathbf{L}_{n-1}\mathbf{K}_{n-1} + \mathbf{R}_{n-1})^{*2}$.*

(ii) *Working modulo $\xi_1, \dots, \xi_{n-1}$, we have $\mathbf{L}_n \equiv 0$ and $\mathbf{R}_n$ is upper triangular with diagonal entries $\xi_n, \xi_n^2, \dots, \xi_n^{2^{n-1}}$.*

(iii)

$$\det(\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n) = \Lambda_{2n}$$

Proof. (i) This follows from the definitions and Lemma 8.2.

(ii) This is entirely straightforward.

(iii) Let δ denote the determinant. From (ii) we can deduce that $\delta \equiv \xi_n^{2^n-1}$ modulo $\xi_1, \dots, \xi_{n-1}$, and in particular it follows that δ is non-zero. Since our relations are homogeneous it follows that δ is a homogeneous polynomial, and we see that it has degree $2^{2n}-1$. Multiplying both sides of the matrix equation 8.3 by the matrix $(\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n)^{\mathrm{cof}}$ of cofactors we see that

$$\begin{pmatrix} \delta c_n \\ \vdots \\ \delta c_{2n-1}\end{pmatrix} = (\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n)^{\mathrm{cof}}\left(\begin{pmatrix} \xi_{2n} \\ \vdots \\ \xi_{n+1}^{2^{n-1}}\end{pmatrix} + \mathbf{L}_n\mathbf{E}_n\right)$$

This shows that for any i with $n \le i \le 2n-1$, the element δ belongs to the ideal J_i of Lemma 10.3 and consequently, on grounds of degree, $\delta = \Lambda_{2n}$. □

We also have Lemma 13.8, relating the Dickson invariants $c_{2n-1}, \dots, c_n$ and the squares $d_{2n-1}^2, \dots, d_n^2$ of our fundamental orthogonal invariants. We use this in order to replace all the c's with d's. Using Lemma 13.8, we obtain the following matrix equation of relations:

$$(\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n)\,\mathbf{J}_n^{*2}\begin{pmatrix} d_n^2 \\ \vdots \\ d_{2n-1}^2\end{pmatrix} = \begin{pmatrix} \xi_{2n} \\ \vdots \\ \xi_{n+1}^{2^{n-1}}\end{pmatrix} + \mathbf{L}_n\mathbf{E}_n + (\mathbf{L}_n\mathbf{K}_n + \mathbf{R}_n)\,\mathbf{F}_n$$

At this stage, the first relation simply gives expression for ξ_{2n} in terms of other generators. So we throw away this relation and throw away the redundant ξ_{2n}. In matrix form the situation can be summarized by omitting the first rows of chosen

matrices.

$$\left(\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n\right)\mathbf{J}_n^{*2}\begin{pmatrix} d_n^2 \\ \vdots \\ d_{2n-1}^2 \end{pmatrix} = \begin{pmatrix} \xi_{2n-1}^2 \\ \vdots \\ \xi_{n+1}^{2^{n-1}} \end{pmatrix} + \mathbf{L}'_n\mathbf{E}_n + \left(\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n\right)\mathbf{F}_n.$$

Notice that the only entries of $\mathbf{L}'_n$ which are not squares are the entries in the first column. Since $\mathbf{K}_n$ begins with a row of zeroes, the first column of $\mathbf{L}'_n$ makes no impact on the product $\mathbf{L}'_n\mathbf{K}_n$ and this matrix has square entries. More precisely we have

$$\mathbf{L}'_n\mathbf{K}_n = \begin{pmatrix} \mathbf{L}_{n-1}^{*2}\mathbf{K}_{n-1}^{*2} & \mathbf{L}_{n-1}^{*2}\mathbf{E}_{n-1}^{*2} \end{pmatrix}$$

Moreover, $\mathbf{R}'_n$ also has square entries. Therefore the left hand side of our matrix equation consists entirely of squares. On the right hand side, the first vector comprises squares. We understand much less about the remaining vector

$$\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n,$$

but it must of course consist of elements which are squares in the ambient ring S. Since this mysterious vector is a column of polynomials in $\xi_0, \ldots, \xi_{2n-1}$ it follows that its entries are squares within the ring $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$ by Lemma 10.4(i). Hence we can take the square root of our matrix equation to obtain what we shall call

14.5. The fundamental system of relations for $S^{O(V)}$:

$$((\mathbf{L}_{n-1}\mathbf{K}_{n-1} \quad \mathbf{L}_{n-1}\mathbf{E}_{n-1}) + \sqrt{\mathbf{R}'_{\mathbf{n}}})\mathbf{J}_n\begin{pmatrix} d_n \\ \vdots \\ d_{2n-1} \end{pmatrix} = \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \end{pmatrix} + \sqrt{\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n}$$

We wish to reorganise this matrix equation in two different ways. First, we wish to describe the relations so that d_{2n-1} appears on the right hand side. To this end, let $\mathbf{G}_{n-1}$ denote the last column of the matrix

$$\left((\mathbf{L}_{n-1}\mathbf{K}_{n-1} \quad \mathbf{L}_{n-1}\mathbf{E}_{n-1}) + \sqrt{\mathbf{R}'_{\mathbf{n}}}\right)\mathbf{J}_n$$

and let $\mathbf{S}_{n-1}$ denote the $(n-1)\times(n-1)$ matrix obtained by deleting this column. Then we can write

14.6. The left handed reorganization:

$$\mathbf{S}_{n-1}\begin{pmatrix} d_n \\ \vdots \\ d_{2n-2} \end{pmatrix} = \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \end{pmatrix} + \sqrt{(\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n)} + \mathbf{G}_{n-1}d_{2n-1}$$

Since $\mathbf{J}_n$ is upper uni-triangular, and also the matrix obtained by deleting the last column of $\mathbf{R}'_n$ is $\mathbf{R}_{n-1}^{*2}$, it follows that

$$\mathbf{S}_{n-1} = (\mathbf{L}_{n-1}\mathbf{K}_{n-1} + \mathbf{R}_{n-1})\mathbf{J}''_n,$$

where $\mathbf{J}''_n$ is the matrix obtained by deleting the last row and last column of $\mathbf{J}_n$. Notice that $\mathbf{J}''_n$ is upper uni-triangular and therefore by Lemma 14.4(iii).

LEMMA 14.7.

$$\det \mathbf{S}_{n-1} = \det (\mathbf{L}_{n-1}\mathbf{K}_{n-1} + \mathbf{R}_{n-1}) = \Lambda_{2n-2}$$

Secondly we wish to describe the relations so that d_n appears on the right hand side of the equation. To do this, let $\mathbf{H}_{n-1}$ denote the first column of the matrix

$$\left((\mathbf{L}_{n-1}\mathbf{K}_{n-1} \quad \mathbf{L}_{n-1}\mathbf{E}_{n-1}) + \sqrt{\mathbf{R}'_{\mathbf{n}}}\right)\mathbf{J}_n$$

and let $\mathbf{T}_{n-1}$ denote the $(n-1)\times(n-1)$ matrix obtained by deleting this column. Then we can write

14.8. The right handed reorganization:

$$\mathbf{T}_{n-1}\begin{pmatrix} d_{n+1} \\ \vdots \\ d_{2n-1}\end{pmatrix} = \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}}\end{pmatrix} + \sqrt{(\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n)} + \mathbf{H}_{n-1}d_n.$$

We have the following result:

LEMMA 14.9.

$$\det \mathbf{T}_{n-1} = \Omega^-_{2n-2}(\xi_0).$$

Proof. Modulo $\xi_0, \ldots, \xi_{n-1}$, $\mathbf{T}_{n-1}$ is upper triangular with diagonal entries $\xi_n, \xi_n^2, \ldots, \xi_n^{2^{n-2}}$ and therefore $\det \mathbf{T}_{n-1}$ is non-zero. We also see that $\det \mathbf{T}_{n-1}$ is homogeneous of degree $(2^n+1)(2^{n-1}-1) = 2^{2n-1} - 2^{n-1} - 1 = \deg \Omega^-_{2n-2}(\xi_0)$. When we invert $\det \mathbf{T}_{n-1}$, we can solve the relations to give expressions for $d_{n+1}, \ldots, d_{2n-1}$ in terms of $\xi_0, \ldots, \xi_{2n-1}, d_n$. Therefore $\det \mathbf{T}_{n-1}$ belongs to the ideal of Corollary 13.7(i) and hence the result follows. □

This concludes our investigation of the subring T.

14.10. Returning to work in T^*. We consider an abstract polynomial ring in $3n$ generators:

$$T^* := \mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}, d_{2n-1}, \ldots, d_n].$$

By using the same symbols ξ_i, d_j as for the subring T we risk great confusion. We shall maintain a clear distinction between our work in T^* and T. The relations we found holding in T can be interpreted as *relators* in T^*. There are $n-1$ of these relators and they are expressed by the column vector

$$\begin{pmatrix} r_1 \\ \vdots \\ r_{n-1}\end{pmatrix} = \left((\mathbf{L}_{n-1}\mathbf{K}_{n-1} \quad \mathbf{L}_{n-1}\mathbf{E}_{n-1}) + \sqrt{\mathbf{R}'_{\mathbf{n}}}\right)\mathbf{J}_n \begin{pmatrix} d_n \\ \vdots \\ d_{2n-1}\end{pmatrix} + \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}}\end{pmatrix} + \sqrt{\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n}.$$

Notice that since $\mathbf{L}'_n \equiv 0$ modulo $\xi_1, \ldots, \xi_{n-1}$ we therefore have the simplification

$$\begin{pmatrix} r_1 \\ \vdots \\ r_{n-1} \end{pmatrix} \equiv \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \end{pmatrix} + \sqrt{\mathbf{R}'_n \mathbf{F}_n},$$

modulo $d_n, \ldots, d_{2n-1}, \xi_1, \ldots, \xi_{n-1}$. Modulo $\xi_1, \ldots, \xi_n$, the last row of $\mathbf{R}'_n$ is zero and hence

$$r_{n-1} \equiv \xi_{n+1}^{2^{n-2}}.$$

More generally for $j \geq 1$, the last j rows of $\mathbf{R}'_n$ are zero modulo $\xi_1, \ldots, \xi_{n+j-1}$ and therefore

$$r_{n-j} \equiv \xi_{n+j}^{2^{n-j}}.$$

This has the crucial consequence that

LEMMA 14.11. *The sequence*

$$d_n, \ldots, d_{2n-1}, \xi_0, \xi_1, \ldots, \xi_{n-1}, \xi_n, r_{n-1}, r_{n-2}, \ldots, r_1$$

is a regular sequence in T^*.

Proof. We manage regular sequences of homogeneous elements in a graded commutative ring using three simple devices:

- Permuting the terms of a regular sequence yields a regular sequence.
- Replacing the last term of a regular sequence by a proper power yields a regular sequence. In view of the first device, we can in fact replace any term of a regular sequence by a proper power.
- If $a_1, \ldots, a_j, \ldots, a_k$ is a regular sequence and b is any ring element such that the ideals $(a_1, \ldots, a_{j-1}, a_j)$ and $(a_1, \ldots, a_{j-1}, b)$ are equal then the sequence obtained by replacing a_j by b is a regular sequence.

These facts are all simple consequences of the definition that a sequence $a_1, \ldots, a_k$ is regular if and only if each term is a non-zero-divisor modulo its predecessors. In T^* we surely have the regular sequence

$$d_n, \ldots, d_{2n-1}, \xi_0, \xi_1, \ldots, \xi_{n-1}, \xi_n, \xi_{n+1}, \xi_{n+2}, \ldots, \xi_{2n-1}$$

and since $r_1 \equiv \xi_{2n-1}$ modulo $d_n, \ldots, d_{2n-1}, \xi_1, \ldots, \xi_{2n-2}$ it follows that we can adjust the last term: so

$$d_n, \ldots, d_{2n-1}, \xi_0, \xi_1, \ldots, \xi_{n-1}, \xi_n, \xi_{n+1}, \xi_{n+2}, \ldots, \xi_{2n-2}, r_1$$

is a regular sequence. Therefore we can replace the penultimate term by its square and

$$d_n, \ldots, d_{2n-1}, \xi_0, \xi_1, \ldots, \xi_{n-1}, \xi_n, \xi_{n+1}, \xi_{n+2}, \ldots, \xi_{2n-2}^2, r_1$$

is also a regular sequence. Since $r_2 \equiv \xi_{2n-2}^2$ modulo $d_n, \ldots, d_{2n-1}, \xi_1, \ldots, \xi_{2n-3}$ we see that

$$d_n, \ldots, d_{2n-1}, \xi_0, \xi_1, \ldots, \xi_{n-1}, \xi_n, \xi_{n+1}, \xi_{n+2}, \ldots, \xi_{2n-3}, r_2, r_1$$

is a regular sequence. Now we replace ξ_{2n-3} by ξ_{2n-3}^4 and then by r_3. Continuing in this way the desired conclusion follows. □

The relators all belong to the kernel of the natural surjection

$$T^* \to T.$$

Thus we have an induced map

$$T^*/(r_1, \ldots, r_{n-1}) \to T.$$

It is our aim to prove that this is an isomorphism and simultaneously that T is integrally closed. We shall use Proposition 1.1. More precisely, we shall show that

LEMMA 14.12. (i) $\Lambda_{2n-2}, \Omega^-_{2n-2}(\xi_0)$ *is a regular sequence in* $T^*/(r_1, \ldots, r_{n-1})$*;*
(ii) *the localizations*

$$T^*/(r_1, \ldots, r_{n-1})\big[\Lambda_{2n-2}^{-1}\big],$$

$$T^*/(r_1, \ldots, r_{n-1})[\Omega^-_{2n-2}(\xi_0)^{-1}]$$

are unique factorization domains;
(iii) Λ_{2n-2} *generates a prime ideal in* $T^*/(r_1, \ldots, r_{n-1})[\Omega^-_{2n-2}(\xi_0)^{-1}]$*; and*
(iv) $\Omega^-_{2n-2}(\xi_0)$ *generates a prime ideal in* $T^*/(r_1, \ldots, r_{n-1})\big[\Lambda_{2n-2}^{-1}\big]$.

Proof. Note that to avoid excessive notation we are now in the position that the names of elements do not tell you which ring they belong to. When we write about the elements $\Lambda_{2n-2}, \Omega^-_{2n-2}(\xi_0)$, keep in mind that the subring of S generated by $\xi_0, \ldots, \xi_{2n}$ is isomorphic to the abstract polynomial ring on $\xi_0, \ldots, \xi_{2n}$ because these elements are algebraically independent in S. Here we are interested in viewing these polynomials in T^* which is defined to be an abstract polynomial ring, and then in the quotient $T^*/(r_1, \ldots, r_{n-1})$ which sits in between T^* and S as follows:

$$T^* \to T^*/(r_1, \ldots, r_{n-1}) \to T \subset S.$$

Therefore there is no real risk of confusion when considering a polynomial in the ξ's so long as we keep clear which of the above rings is relevant at each point of argument.

(i) We know from Lemma 14.11 that

$$\xi_1, \ldots, \xi_n$$

is a regular sequence in the quotient ring $T^*/(r_1, \ldots, r_{n-1})$. Therefore

$$\xi_1, \ldots, \xi_{n-1}, \xi_n^{2^{n-1}-1}$$

is also a regular sequence. By Corollary 13.3 we have that $\Omega^-_{2n-2}(\xi_0) \equiv \xi_n^{2^{n-1}-1}$ modulo $\xi_1, \ldots, \xi_{n-1}$ and therefore

$$\xi_1, \ldots, \xi_{n-1}, \Omega^-_{2n-2}(\xi_0)$$

is a regular sequence, and so also is

$$\xi_1, \ldots, \xi_{n-2}, \xi_{n-1}^{2^{n-1}-1}, \Omega^-_{2n-2}(\xi_0).$$

Using the fact that $\Lambda_{2n-2} \equiv \xi_{n-1}^{2^{n-1}-1}$ modulo $\xi_1, \ldots, \xi_{n-2}$ we see that

$$\xi_1, \ldots, \xi_{n-2}, \Lambda_{2n-2}, \Omega^-_{2n-2}(\xi_0)$$

is a regular sequence. (In fact, since ξ_0 involves the extra variable x_0 we can even say that

$$\xi_0, \xi_1, \ldots, \xi_{n-2}, \Lambda_{2n-2}, \Omega^-_{2n-2}(\xi_0)$$

is a regular sequence.) In particular

$$\Lambda_{2n-2}, \Omega^-_{2n-2}(\xi_0)$$

is a regular sequence in $T^*/(r_1, \ldots, r_{n-1})$ as claimed.

(ii) First notice from the left handed reorganization (14.6) that when we invert

$$\det \mathbf{S}_{n-1} = \Lambda_{2n-2}$$

the relations can be solved to express $d_n, \ldots, d_{2n-2}$ in terms of $\xi_0, \ldots, \xi_{2n-1}$ and d_{2n-1}. This gives the isomorphism

$$T^*/(r_1, \ldots, r_{n-1})\big[\Lambda_{2n-2}^{-1}\big] \cong \mathbb{F}_2\big[\xi_0, \ldots, \xi_{2n-1}, d_{2n-1}, \Lambda_{2n-2}^{-1}\big]$$

and we can see on grounds of Krull dimension that this ring is a localized polynomial ring; in particular it is a unique factorization domain. Similarly, from the right handed reorganization (14.8) we deduce the isomorphism

$$T^*/(r_1, \ldots, r_{n-1})[\Omega^-_{2n-2}(\xi_0)^{-1}] \cong \mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}, d_n, \Omega^-_{2n-2}(\xi_0)^{-1}],$$

because inverting $\det \mathbf{T}_{n-1} = \Omega^-_{2n-2}(\xi_0)$ allows us to solve for $d_{n+1}, \ldots, d_{2n-1}$ in terms of $\xi_0, \ldots, \xi_{2n-1}, d_n$, and this ring is also a localized polynomial ring; in particular it is a unique factorization domain.

Finally (iii) and (iv) hold because Λ_{2n-2} and $\Omega^-_{2n-2}(\xi_0)$ are irreducible polynomials in the ring $\mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$. □

In view of Proposition 1.1, this completes the calculation of the ring of invariants $S^{O(V)}$.

15. The invariants for O^-. Let ξ_- be any quadratic form of $-$type. Then $\xi_0 + \xi_- = x_-^2$ for some fixed $x \in V^* \setminus U^*$. The composite $\operatorname{Ker} x \to V \to U$ is an isomorphism and so we identify $\operatorname{Ker} x$ with U. We write O^- for the group of automorphisms of (U, ξ_-)

We show that $S(U^*)^{O^-}$ is given up to isomorphism by adding the single additional relation $P^-(0) = 0$ to the ring of invariants $S^{O(V)}$. Let's see what happens when we adjoin this additional relation to our presentation. This simply amounts to setting $d_n = 0$.

Note that ξ_- belongs to $S(U^*)$ and in just the same way as for Lemma 8.5 we have

LEMMA 15.1. *The elements $\xi_-, \xi_1, \ldots, \xi_{2n-1}$ are algebraically independent in $S(U^*)$.*

Moreover, Corollary 13.4 simplifies in a significant way:

LEMMA 15.2. *For each j,*

$$Sq^j(\Omega^-_{2n-2}(\xi_-)) = \Omega^-_{2n-2}(\xi_-)P_j$$

where P_j is the coefficient of degree j in the restriction of $P^-(t)$ to U^*.

We begin by studying the subring T of $S(U^*)$ generated by the $3n-1$ elements

$$\xi_-, \xi_1, \ldots, \xi_{2n-1}, d_{2n-1}, \ldots, d_{n+1}.$$

We shall in due course see that $T = S(U^*)^{O^-}$.

The fundamental system of relations for $S^{O(V)}$ now simplify in line with (14.8):

15.3. The fundamental system of relations for O^-.

$$\mathbf{T}_{n-1}\begin{pmatrix} d_{n+1} \\ \vdots \\ d_{2n-1} \end{pmatrix} = \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \end{pmatrix} + \sqrt{(\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n)}.$$

Direct inspection of $\mathbf{T}_{n-1}$ reveals that its top right hand entry is of the form

$$\xi_{2n-2} + \text{ terms involving } \xi_0, \ldots, \xi_{2n-3}.$$

It follows that the $(n-2)\times(n-2)$ matrix $\mathbf{T}''_{n-1}$ found by deleting the first row and last column of $\mathbf{T}_{n-1}$ has determinant $\Omega^-_{2n-4}(\xi_0)^2$. Since the first relation simply gives expression for ξ_{2n-1} in terms of the other generators we can dispense with this relation, throw out ξ_{2n-1}, and use

15.4. The reduced system of relations for O^-.

$$\mathbf{T}''_{n-1}\begin{pmatrix} d_{n+1} \\ \vdots \\ d_{2n-2} \end{pmatrix} = \begin{pmatrix} \xi_{2n-2} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \end{pmatrix} + \sqrt{(\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n)} + \mathbf{G}'_{n-1}d_{2n-1}.$$

This concludes our analysis of the subring T. Now we consider an abstract polynomial ring on generators

$$\xi_-, \xi_1, \ldots, \xi_{2n-1}, d_{2n-1}, \ldots, d_{n+1}.$$

The matrix relation (15.3) can be interpreted as providing a sequence of relators $r_1, \ldots, r_{n-1}$ in T^* so that there is a natural map

$$T^*/(r_1, \ldots, r_{n-1}) \to T.$$

As before, $r_1, \ldots, r_{n-1}$ form part of a longer regular sequence. This time

15.5. The fundamental regular sequence is

$$d_{n+1}, \ldots, d_{2n-1}, \xi_-, \xi_1, \ldots, \xi_n, r_{n-1}, \ldots, r_1.$$

In a simple variation on the odd dimensional case we have

LEMMA 15.6. (i) *The sequence*

$$\Omega^-_{2n-4}(\xi_-), \Omega^-_{2n-2}(\xi_-)$$

is a regular sequence in $T^*/(r_1, \ldots, r_{n-1})$,

(ii) *the localizations*

$$T^*/(r_1, \ldots, r_{n-1})[\Omega^-_{2n-4}(\xi_-)^{-1}]$$
$$T^*/(r_1, \ldots, r_{n-1})[\Omega^-_{2n-2}(\xi_-)^{-1}]$$

are isomorphic to the localized polynomial rings

$$\mathbb{F}_2[\xi_-, \xi_1, \ldots, \xi_{2n-2}, d_{2n-1}, \Omega^-_{2n-4}(\xi_-)^{-1}]$$
$$\mathbb{F}_2[\xi_-, \xi_1, \ldots, \xi_{2n-2}, \xi_{2n-1}, \Omega^-_{2n-2}(\xi_-)^{-1}]$$

respectively, and so these are unique factorization domains,

(iii) $\Omega^-_{2n-4}(\xi_-)$ *is irreducible in*

$$\mathbb{F}_2[\xi_-, \xi_1, \ldots, \xi_{2n-2}, \xi_{2n-1}, \Omega^-_{2n-2}(\xi_-)^{-1}]$$

and $\Omega^-_{2n-2}(\xi_-)$ *is irreducible in*

$$\mathbb{F}_2[\xi_-, \xi_1, \ldots, \xi_{2n-2}, d_{2n-1}, \Omega^-_{2n-4}(\xi_-)^{-1}].$$

Proposition 1.1 now comes into force and we deduce that $T^*/(r_1, \ldots, r_{n-1})$ is isomorphic to the subring T and that this is the ring of invariants as required.

16. The invariants for O^+. It is useful now to have formulations of Corollaries 13.4 and 13.5 for $P^+(t)$. These are as follows and are proved in exactly the same way.

COROLLARY 16.1. *Let $j \geq 0$ be a natural number and let P^+_j be the coefficient of degree j in $P^+(t)$, (i.e. P^+_j is the coefficient of $t^{2^{2n-1}+2^{n-1}-j}$). Let P''_j be the coefficient of degree $j-1$ in $\Omega^+_{2n-2}(t^2+\xi_0)$, (i.e. P''_j is the coefficient of $t^{2^{2n-1}+2^{n-1}-j}$). Then*

$$Sq^j\Omega^+_{2n-2}(\xi_0) = \Omega^+_{2n-2}(\xi_0)P^+_j + P''_jP^+(0).$$

COROLLARY 16.2. $(\Omega^+_{2n-4}(\xi_0))^2\xi_{2n-1} + \Omega^+_{2n-2}(\xi_0)d_{2n-1} + \Lambda_{2n-2}P^+(0)$ *belongs to the subring generated by* $\xi_0, \ldots, \xi_{2n-2}$

We shall have need of the following embellishment of our discussion of the odd dimensional case.

LEMMA 16.3. *There exist polynomials* $f_0, \ldots, f_n \in \mathbb{F}_2[\xi_0, \ldots, \xi_{2n-1}]$ *such that*

$$P^+(0) = \sum_{\ell=0}^{n-1} f_\ell d_{n+\ell} + f_n$$

and which satisfy the conditions $f_0 = \xi_0^{2^{n-1}}$, *and in general for* $1 \leq j \leq n$ *we have* $f_j \equiv \xi_j^{2^{n-1}}$ *modulo* $\xi_0, \ldots, \xi_{j-1}$.

Proof. Since $P^+(0)^2 = Q^+(\xi_0)$ we see from Proposition 13.1 that

$$P^+(0)^2 = \sum_{\ell=0}^{n} c_{n+\ell}(\alpha_\ell^+(\xi_0))^{2^{n-\ell}},$$

and in addition that modulo $\xi_0, \xi_1, \ldots, \xi_{j-1}$

$$P^+(0)^2 \equiv \xi_j^{2^n} c_{n+j} + \text{ terms involving Dickson invariants of lower degree.}$$

From this we can deduce that

$$P^+(0) \equiv \xi_j^{2^{n-1}} d_{n+j} + \text{ terms involving } d\text{'s of lower degree.}$$

and the result follows. □

We now choose a quadratic form ξ_+ on U of +type. As in the −type case, there is a vector $x_+ \in V^* \setminus U^*$ such that $\xi_+ = \xi_0 + x_+^2$. The composite of inclusion and restriction supplies an isomorphism between $\operatorname{Ker} x_+$ and U^* so we identify these two. On restriction to $\operatorname{Ker} x_+$ there is a new relation, namely $P^+(0) = 0$.

The identification $\operatorname{Ker} x_+ = U^*$ gives us a map

$$S \to S(U^*)$$

which carries the invariants of $O(V)$ into the ring of invariants of O^+. Therefore we wish to stick with the choice of d_j as key generators for the new ring of invariants even though it may at first appear that working with coefficients chosen from $P^+(t)$ would be more natural. In fact it makes very little difference because of Lemma 13.10. From Lemma 16.3 we see that this is linear in the d's with coefficients $f_0, \ldots, f_{n-1}$ and we adjoin the row of f's as an additional last row to the matrix

$$((\mathbf{L}_{n-1}\mathbf{K}_{n-1} \quad \mathbf{L}_{n-1}\mathbf{E}_{n-1}) + \sqrt{\mathbf{R}'_{\mathbf{n}}})\mathbf{J}_n$$

at the left of the fundamental relations for $O(V)$ in (14.5). This yields an $n \times n$ matrix $\mathbf{M}_n$ and allows us to write the relations we have found for the group O^+ in the form

$$\mathbf{M}_n \begin{pmatrix} d_n \\ \vdots \\ d_{2n-1} \end{pmatrix} = \begin{pmatrix} \xi_{2n-1} \\ \vdots \\ \xi_{n+1}^{2^{n-2}} \\ \\ \xi_n^{2^{n-1}} \end{pmatrix} + \begin{pmatrix} \sqrt{\mathbf{L}'_n\mathbf{E}_n + (\mathbf{L}'_n\mathbf{K}_n + \mathbf{R}'_n)\mathbf{F}_n} \\ \\ \xi_n^{2^{n-1}} + f_n \end{pmatrix}.$$

A variation on the arguments we have used before leads to the conclusion that

$$\det \mathbf{M}_n = \Omega^+_{2n-2}(\xi_+)$$

and that

$$\det \mathbf{M}''_n = \Omega^+_{2n-4}(\xi_+)^2$$

where $\mathbf{M}''_n$ is the matrix obtained by omitting the first row and last column of $\mathbf{M}_n$. The same regular sequence arguments can be applied, and the ring of invariants for O^+ is established.

ACKNOWLEDGEMENT. The first author wishes to acknowledge his collaboration with David Carlisle during the mid nineteen-eighties when the calculations described here were first studied.

REFERENCES

1. J. F Adams, 2-tori in E_8, *Math. Ann.* **278** (1987), 29–39.

2. D. J. Benson, *Polynomial invariants of finite groups,* London Math. Soc. Lecture Note Series No. 190 (Cambridge University Press, 1993).

3. D. J. Benson and W. W. Crawley-Boevey, A ramification formula for Poincaré series, and a hyperplane formula in modular invariant theory, *Bull. London Math. Soc.* **27** (1995), 435–440.

4. P. J. Cameron, *Projective and polar spaces,* Queen Mary Maths. Notes **13** (1991), http://www.maths.qmul.ac.uk/∼pjc/pps/

5. 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** (1911), 75–98.

6. M. Domokos and P. E. Frenkel, On orthogonal invariants in characteristic 2, preprint arXiv:math. RA/0303106 v2, 13 September 2003.

7. S. Kochman, An algebraic filtration of H_*BO, in *Northwestern Homotopy Theory Conference (Evanston, Illinois, 1982), Contemporary Math.* **19** (1983), 115–143.

8. H. Matsumura, *Commutative ring theory*, Cambridge Stud. Adv. Math **8** (1980).

9. A. Neeman, The connection between a conjecture of Carlisle and Kropholler, now a theorem of Benson and Crawley-Boevey, and Grothendieck's Riemann-Roch and duality theorems, *Comment. Math. Helvetici* **70** (1995), 339–349.

10. M. Neusel, The invariants of the symplectic groups (Appenzell 1998), http://hopf.math.purdue.edu/cgi-bin/generate?/Neusel/symplectic.

11. S. Mohseni-Rajaei, *Rational invariants of orthogonal groups over finite fields*, PhD Thesis, Queen Mary College, University of London, 1997.

12. S. Mohseni-Rajaei, Rational invariants of certain orthogonal groups over finite fields of characteristic two. *Comm. Algebra* **28** (2000), 2367–2393.

13. L. Smith, *Polynomial invariants of finite groups,* (A. K. Peters, 1995).

14. A. Steel, Calculation of the factors of $\Omega_6(X)$ using Magma, Private communication, June 2002, http://www.maths.gla.ac.uk/∼phk/Steel.htm.

15. N. E. Steenrod and D. B. A. Epstein, *Cohomology Operations, Annals of Maths Studies* No. 50, (Princeton University Press, 1974).

16. R. Stong, Determination of $H^*(BO(k, \ldots, \infty), Z_2)$ and $H^*(BU(k, \ldots, \infty), Z_2)$, *Trans. Amer. Math. Soc.* **107** (1963), 526–544.

17. F. Voloch, A ramification formula for modular Poincaré series, private communication, 1985.

18. C. W. Wilkerson, A Primer on the Dickson Invariants, **in:** Proc. Northwestern Homotopy Theory Conference, *Contemp. Math.* **19** (1983), 421–434; as corrected at the Hopf Topology Archive http://hopf.math.purdue.edu/pub/hopf.html.

19. C. W. Wilkerson, Lab Notes on the exceptional Lie group E_8 at the prime 2, (preprint, Purdue, 2000).

20. W. Wu, Les i-carrés dans une variété grassmannienne, *C.R. Acad. Sci. Paris* **230** (1950), 918–920.