CHERN CLASSES AND THE EXTRASPECIAL p-GROUP OF ORDER p^5 AND EXPONENT p

David J. Green

Inst. f. Exp. Math., Univ. GH Essen, Ellernstr. 29
D–45326 Essen, Germany

17 September 1996

ABSTRACT

For p an odd prime, the cohomology ring of the extraspecial p-group of order p^5 and exponent p is investigated. A presentation is obtained for the subquotient generated by Chern classes, modulo nilradical.

Moreover, it is proved that, for every extraspecial p-group of exponent p, the top Chern classes of the irreducible representations do not generate the Chern subring modulo nilradical. Finally, a related question about symplectic invariants is discussed, and is solved for $Sp_4(\mathbb{F}_p)$.

INTRODUCTION

Almost all techniques for calculating the cohomology ring of an arbitrary finite group assume prior knowledge of the cohomology of its Sylow p-subgroups. But calculating the cohomology ring of a p-group is very difficult. The one general method is the Lyndon–Hochschild–Serre spectral sequence of a group extension, but this can be intractible even in very simple cases.

One family of p-groups that illustrate this difficulty particularily well are the extraspecial p-groups of exponent p. One would expect these groups to be well-behaved cohomologically: their proper quotients are all elementary abelian, and their automorphism groups are unusually large. Also, the cohomology of the extraspecial 2-groups was calculated elegantly by Quillen [**8**]. However, even for the extraspecial p-group of order p^3 and exponent p, the spectral sequence of the central extension is intractible.

New techniques to compute the cohomology rings of p-groups are therefore needed, and the extraspecial p-groups are important test cases.

For this reason, many people have investigated the cohomology of the extraspecial p-groups, and have applied it to such questions as convergence of spectral sequences and modules with periodic resolutions of large period.

For $n \geq 1$ and p an odd prime, denote by P_n the extraspecial p-group p_+^{1+2n} of order p^{2n+1} and exponent p. Much of the attention has focused on the smallest group P_1, because its cohomology is known. (See the papers [**7**], [**6**] for integral and mod-p cohomology respectively). All generators of the mod-p cohomology ring can be given concrete descriptions: degree 1 elements represent homomorphisms from the group to $\mathbb{F}_p$, and the other generators can be described as transfers from proper subgroups, as images of the Bockstein map, as Massey products, or as Chern classes of group representations.

Now let us consider the mod-p cohomology ring of an arbitrary extraspecial p-group. Tezuka and Yagita have shown that this has the same prime ideal spectrum as the subring generated by top Chern classes [**9**]. So it is very reasonable to ask whether all generators of the cohomology ring can be described using standard constructions such as transfer, Evens norm and Chern classes. Irrespective of the answer to this question, it is worth our while to investigate the subring generated by classes that can be thus described.

To study such a subring, we also need to be able to tell whether or not a given cohomology class is zero. We therefore restrict our attention to cohomology rings modulo their nilradicals: by a well-known theorem of Quillen (Theorem 6.2 here), non-nilpotent cohomology classes are detected by their restrictions to elementary abelian subgroups.

Modulo nilradical, the integral cohomology of P_1 is generated by Chern classes of group representations. The same holds for mod-p cohomology, unless $p = 3$. Combining these facts with the result of Tezuka and Yagita mentioned above, it becomes clear that the Chern subring modulo nilradical is a very important subquotient of the cohomology ring of an extraspecial p-group.

The purpose of this paper is to obtain a presentation of this subquotient for the extraspecial p-group of order p^5 and exponent p. This paper therefore carries on from paper [**5**], where the subquotient was studied for arbitrary extraspecial p-groups, and several formulae were obtained. After establishing the main result, some corollaries are obtained. For arbitrary extraspecial p-groups, the containment of the ring generated by top Chern classes in the Chern subring modulo nilradical is shown to be strict. The main problem of this paper gives rise to a natural question about symplectic invariants: this is discussed, and one case is answered using the result.

By employing a suitable partition of the set of maximal elementary abelian subgroups, the search for relations in the Chern subring may be pursued in a methodical fashion. The extraspecial p-group P_{n+1} is the central product $P_1 * P_n$. As a result, there is a cohomology inflation map from P_{n+1} to $P_1 \times P_n$. Some maximal elementary abelian subgroups of P_{n+1} lift to elementary abelian subgroups of $P_1 \times P_n$, and some do not: this is the partition. There is one additional property of P_2 that allows us to obtain a presentation of its Chern subring modulo nilradical. Every element of the Chern subring can be approximated by an element of the Tezuka–Yagita subring, in such a way that the difference (the Δ of Definition 3.2) is detected by the inflation map.

This technique lends itself to a number of generalizations that could be used to launch an attack by induction on the Chern subrings of all extraspecial groups. It is to be hoped that further research will identify the correct generalization for this task.

The task of obtaining the Chern subring modulo nilradical for P_2 can be easily abstracted into a purely algebraic problem. The main part of the paper is taken up in solving this algebraic problem.

PROBLEM 0.1. *For an odd prime p and a positive integer n, let E_n be a $2n$-dimensional $\mathbb{F}_p$-vector space, carrying a nondegenerate symplectic bilinear form. Let $K_0, \ldots, K_{n-1}$ be indeterminates, and let F_n denote the polynomial algebra $S(E_n^*) \otimes_{\mathbb{F}_p} \mathbb{F}_p[K_0, \ldots, K_{n-1}]$.*

For each maximal totally isotropic subspace I of E_n, there is then a unique algebra homomorphism $q_I \colon F_n \to S(I^*)$ which behaves on E_n^* as the restriction map $E_n^* \to I^*$, and sends K_r to $D_r(I^*)$, the Dickson invariant in the $(p^n - p^r)$th symmetric power of I^*.

The intersection of the kernels of all the q_I is an ideal in F_n; define $\mathcal{Q}_n$ to be the corresponding quotient algebra. Give a presentation for $\mathcal{Q}_n$.

A presentation for $\mathcal{Q}_2$ is achieved in Theorem 5.7. After that, we shall prove in Theorem 6.3 that the Chern subring modulo nilradical for P_2 is isomorphic to $\mathcal{Q}_2 \otimes_{\mathbb{F}_p} \mathbb{F}_p[Z]$ for an indeterminate Z. Together, these constitute the main result of the paper.

1. A REGULAR SEQUENCE

Let b denote the symplectic form $E_n \otimes_{\mathbb{F}_p} E_n \to \mathbb{F}_p$, and denote by q the quotient map $F_n \to \mathcal{Q}_n$. Then, for each maximal totally isotropic subspace I of E_n, there is a unique map $\hat{q}_I \colon \mathcal{Q}_n \to S(I^*)$ such that $\hat{q}_I q = q_I$.

Write $\mathcal{T}_n$ for the image of $S(E_n^*)$ under q. Pick a symplectic basis $A_1, \ldots, A_n, B_1, \ldots, B_n$ for E_n: so $A_i \perp A_j$, $B_i \perp B_j$ and $b(A_i, B_j) = \delta_{ij}$. Take the corresponding dual basis $A_1^*, \ldots, A_n^*, B_1^*, \ldots, B_n^*$ for E_n^*. Define elements of $\mathcal{T}_n$ by $\alpha_i = q(A_i^*)$ and $\beta_i = q(B_i^*)$. Then $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ generate $\mathcal{T}_n$ as an $\mathbb{F}_p$-algebra. Denote by $R_r(E_n)$ the element $A_1^* B_1^{*p^r} - A_1^{*p^r} B_1^* + \cdots + A_n^* B_n^{*p^r} - A_n^{*p^r} B_n^*$ of $S(E_n^*)$. If the vector space E_n is clear from the context, this will be shortened to R_r. Note that R_r is the $b(v, F^r(v))$ of [**3**].

THEOREM 1.1. (Tezuka–Yagita) *The sequence $R_1, \ldots, R_n$ in $S(E_n^*)$ is a regular sequence. The ideal generated by these elements contains R_r for all $r \geqslant 1$, and is the kernel of the surjection $S(E_n^*) \to \mathcal{T}_n$.*

Proof. See Proposition 8.2 of [**3**]. The h of that paper is defined to be the codimension in E_n of a maximal totally isotropic subspace, and so takes the value n here. The first two parts are explicitly stated. The last part follows, using the Nullstellensatz, from the fact that the ideal is radical and from the description of the variety in terms of isotropic subspaces. ∎

2. DICKSON INVARIANTS

We now recall the salient facts about the Dickson invariants. See Chapter 8 of Benson's book [**2**] for proofs.

Let V be an m-dimensional $\mathbb{F}_p$-vector space. For each $0 \leqslant r \leqslant m-1$, there is a *Dickson invariant* $D_r(V)$ in the $(p^m - p^r)$th symmetric power of V and

$$\prod_{v \in V} (X - v) = X^{p^m} + \sum_{r=0}^{m-1} (-1)^{m-r} D_r(V) X^{p^r} \quad \text{in } S(V)[X]. \tag{1}$$

The natural action of $GL(V)$ on $S(V)$ has as ring of invariants the polynomial algebra $\mathbb{F}_p[D_0, \ldots, D_{m-1}]$. In several papers, $D_r(V)$ is denoted $c_{m,r}$ or $d_{m,r}$.

Each Dickson invariant is a polynomial in the elements of any basis for V, and the polynomial depends only on p, r and m. If $w_1, \ldots, w_m$ are elements of an $\mathbb{F}_p$-vector space W, and $r < m$, then $D_r(w_1, \ldots, w_m)$ shall denote the evaluation at $(w_1, \ldots, w_m)$ of the polynomial for $D_r(\mathbb{F}_p^m)$. The following lemma relates this to the Dickson invariants of the space spanned by the w_i. It takes a particularly elegant form for dual spaces.

LEMMA 2.1. *Let V be an m-dimensional $\mathbb{F}_p$-vector space, and U a subspace of codimension ℓ. Then, for every $0 \leqslant r \leqslant m-1$,*

$$\mathrm{Res}_U\left(D_r(V^*)\right) = \begin{cases} D_{r-\ell}(U^*)^{p^\ell} & \text{if } \ell \leqslant r, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Obvious from Eqn. (1). ∎

This paper is particularily concerned with small cases. The first three Dickson invariants are easily calculated: $D_0(w) = w^{p-1}$ and

$$D_0(w_1, w_2) = (w_1 {w_2}^p - {w_1}^p w_2)^{p-1} \qquad D_1(w_1, w_2) = \frac{w_1^{p^2-1} - w_2^{p^2-1}}{w_1^{p-1} - w_2^{p-1}} \,. \qquad (2)$$

Note in particular that if we take for any m-dimensional V a non-zero element of each 1-dimensional subspace, and multiply these together, we get an element of $S(V)$ which is well-defined up to a scalar, and has $(p-1)$th power $D_0(V)$. If $m = 2$ and V has basis v_1, v_2, then this element is $v_1 {v_2}^p - {v_1}^p v_2$.

In $\mathcal{Q}_n$, define $\kappa_{n,r} = q(K_r)$ for $0 \leqslant r \leqslant n-1$. Then the α_i, β_j and $\kappa_{n,r}$ together generate the $\mathbb{F}_p$-algebra $\mathcal{Q}_n$. Note that the algebraic independence of the Dickson invariants, together with the definition of q, ensures that the $\kappa_{n,r}$ not only are algebraically independent over $\mathbb{F}_p$ in $\mathcal{Q}_n$, but also, no polynomial in them over $\mathbb{F}_p$ is a zero divisor in $\mathcal{Q}_n$. For small values of n we will abbreviate $\kappa_{n,r}$, denoting $\kappa_{1,0}$, $\kappa_{2,0}$, $\kappa_{2,1}$ by κ, κ_0, κ_1 respectively.

3. PARTITION

The object of this section is to prove a result (Proposition 3.3) which allows the search for relations in $\mathcal{Q}_2$ to be carried out in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. This is achieved by partitioning the set of maximal totally isotropic subspaces of E_2 into two families, and for each family, determining which elements of $\mathcal{Q}_2$ it fails to detect. This partition can in fact be performed in E_n, and so we will only restrict ourselves to E_2 when this becomes necessary.

Suppose that $n = \ell + m$. Then E_n is the orthogonal direct sum $E_n = E_\ell \perp E_m$ of nondegenerate symplectic spaces E_ℓ, E_m. Partition the set of maximal totally isotropic subspaces I of E_n as $\Phi \coprod \Psi$, where $I \in \Phi$ if and only if I is the direct sum of (necessarily maximal) totally isotropic subspaces of E_ℓ and E_m.

LEMMA 3.1. *Let $n = \ell + m$. Then the isomorphism $S(E_n^*) \cong S(E_\ell^*) \otimes S(E_m^*)$ induces an inflation homomorphism $\pi^* \colon \mathcal{Q}_n \to \mathcal{Q}_\ell \otimes \mathcal{Q}_m$ such that, for any $x \in \mathcal{Q}_n$, we have $\pi^*(x) = 0$ if and only if $\hat{q}_I(x) = 0$ for all $I \in \Phi$.*

Proof. As $\mathbb{F}_p^n \cong \mathbb{F}_p^\ell \oplus \mathbb{F}_p^m$ and $GL_\ell(\mathbb{F}_p) \times GL_m(\mathbb{F}_p) \leqslant GL_n(\mathbb{F}_p)$, each $D_r(\mathbb{F}_p^n)$ is a polynomial in the $D_s(\mathbb{F}_p^\ell)$ and the $D_t(\mathbb{F}_p^m)$. Define $\pi^*(\kappa_{n,r})$ to be the corresponding polynomial in the $\kappa_{\ell,s} \otimes 1$ and the $1 \otimes \kappa_{m,t}$. The rest is obvious. ∎

Remark. The above partition is related to the fact that the extraspecial group P_n is the central product $P_\ell * P_m$. The inflation map corresponds to the cohomology inflation from P_n to $P_\ell \times P_m$.

Definition 3.2. For a polynomial $f \in \mathcal{T}_2[x_0, x_1]$ with coefficients in $\mathcal{T}_2$, define $\Delta(f) \in \mathcal{Q}_2$ by

$$\Delta(f) = f(\kappa_0, \kappa_1) - f(D_0(\alpha_1, \beta_1), D_1(\alpha_1, \beta_1)) \, ,$$

and define γ_2 to be the element $D_1(\alpha_1, \beta_1) - D_1(\alpha_2, \beta_2)$ of $\mathcal{T}_2$.

Proposition 3.3. *Let $f \in \mathcal{T}_2[x_0, x_1]$ be a polynomial with coefficients in $\mathcal{T}_2$. Then the element $f(\kappa_0, \kappa_1)$ of $\mathcal{Q}_2$ belongs to $\mathcal{T}_2$ if and only if there exists $t \in \mathcal{T}_2$ such that the equation $\Delta(f) = t\gamma_2$ holds after inflation to $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. If such t does exist, then $\Delta(f) = t\gamma_2$ holds in $\mathcal{Q}_2$.*

Remark. The point here in Definition 3.2 and Proposition 3.3 is that each element of $\mathcal{Q}_2$ can be approximated by an element of $\mathcal{T}_2$ in such a way that the difference (Δ) can be analysed in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$: that is, the difference can be worked with easily. The main obstacle to obtaining a presentation for $\mathcal{Q}_n$ for general n is the current lack of such an approximation by elements of $\mathcal{T}_n$.

Before proving this proposition, we shall establish two auxilliary results. We shall work with the partition associated to the orthogonal direct sum decomposition $E_n = E_1 \perp E_{n-1}$, where $n \geqslant 2$ and E_1 has basis A_1, B_1.

Lemma 3.4. *For $n \geqslant 2$, let I be a maximal totally isotropic subspace of E_n. Then $I \in \Psi$ if and only if the restrictions of α_1 and β_1 are linearly independent in I^*.*

Proof. Obvious. ∎

By the definition of $\mathcal{Q}_n$, the maximal totally isotropic subspaces in Φ and Ψ combined detect every non-zero element of $\mathcal{Q}_n$. We shall now determine the ideals of elements which Φ and Ψ individually fail to detect. Recall that $\mathcal{T}_n \cong S(E_n^*)/(R_1, \ldots, R_n)$.

Lemma 3.5.

1. *The equation* $(\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1)\gamma_n = R_n$ *in* $S(E_n^*)/(R_1,\ldots,R_{n-1})$ *has a unique solution* γ_n*. As in Definition 3.2,* $\gamma_2 = D_1(\alpha_1,\beta_1) - D_1(\alpha_2,\beta_2)$*.*

2. *Consider the ideal in* $\mathcal{T}_n$ *of classes whose image under* $\hat{q}_I$ *is zero for every* $I \in \Phi$*. It is the principal ideal generated by* $\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1$*.*

3. *The corresponding ideal for* Ψ *is also principal; it is generated by* γ_n *(considered as an element of* $\mathcal{T}_n$*).*

Proof. Write $\widehat{\mathcal{T}}$ for $S(E_n^*)/(R_1,\ldots,R_{n-1})$. For part 1, we have $R_r(E_n) = R_r(E_1) + R_r(E_{n-1})$. It follows from the Tezuka–Yagita theorem for E_{n-1} that $R_n(E_n)$ lies in the ideal in $S(E_n^*)$ generated by the $R_r(E_n)$ for $r < n$, and the $R_r(E_1)$ for $r \leqslant n$. Now apply the Tezuka–Yagita theorem again, this time for E_1. Hence (the image of) $R_n(E_n)$ lies in the principal ideal of $\widehat{\mathcal{T}}$ generated by $\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1$. Therefore γ_n exists; it is unique since $R_n(E_n)$ is a non-zero divisor in $\widehat{\mathcal{T}}$. Observing that $(\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1)D_1(\alpha_1,\beta_1) = \alpha_1\beta_1{}^{p^2} - \alpha_1{}^{p^2}\beta_1$, we can verify the equation for γ_2.

For part 2, observe first that $\hat{q}_I(\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1)$ is zero in $S(I^*)$ for every $I \in \Phi$, and non-zero for every $I \in \Psi$. Since $S(I^*)$ is an integral domain, it follows that $\hat{q}_I(\gamma_n) = 0$ in $S(I^*)$ for every $I \in \Psi$. Therefore, if $t \in \mathcal{T}_n$ satisfies $\hat{q}_I(t) = 0$ for every $I \in \Phi$, then $t\gamma_n = 0$ in $\mathcal{T}_n$.

Now pick $\hat{t} \in \widehat{\mathcal{T}}$ lying above t. Then for some $s \in \widehat{\mathcal{T}}$, $\hat{t}\gamma_n = sR_n(E_n)$. Multiplying both sides by $\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1$ and rearranging then yields $(\hat{t} - s(\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1))R_n = 0$. Since R_n is a non-zero divisor, $\hat{t}$ lies in the ideal of $\widehat{\mathcal{T}}$ generated by $\alpha_1\beta_1{}^p - \alpha_1{}^p\beta_1$, proving part 2. The same method works for part 3. ∎

We can now proceed with the proof of Proposition 3.3.

Proof of Proposition 3.3. For $r = 0$ or 1, and $I \in \Psi$, the images under $\hat{q}_I$ of κ_r and $D_r(\alpha_1,\beta_1)$ both equal $D_r(I^*)$. So for every $I \in \Psi$, the images under $\hat{q}_I$ of $f(\kappa_0,\kappa_1)$ and $f(D_0(\alpha_1,\beta_1), D_1(\alpha_1,\beta_1))$ must be equal. Therefore if $f(\kappa_0,\kappa_1) \in \mathcal{T}_2$ then there exists $t \in \mathcal{T}_2$ such that

$$\Delta(f) = t\gamma_2 \,. \tag{3}$$

Conversely, suppose that there is a $t \in \mathcal{T}_2$ such that Eqn. (3) holds after $\hat{q}_I$ for every $I \in \Phi$. Then Eqn. (3) holds in $\mathcal{Q}_2$, since each side of the equation is in $\ker \hat{q}_I$ for every $I \in \Psi$. Hence $f(\kappa_0,\kappa_1) \in \mathcal{T}_2$. ∎

4. TECHNICAL RESULTS

In light of Proposition 3.3, we want a presentation for $\mathcal{Q}_1$. This has generators α_1, β_1 and $\kappa_{1,0}$. We shall drop the subscripts from these generators.

PROPOSITION 4.1. *The $\mathbb{F}_p$-algebra $\mathcal{Q}_1$ is generated by α, β and κ; a sufficient set of relations is $\kappa^2 = \alpha^{2(p-1)} - \alpha^{p-1}\beta^{p-1} + \beta^{2(p-1)}$, $\alpha\kappa - \alpha^p = 0$, and $\beta\kappa - \beta^p = 0$.*

Proof. These relations are easily verified after every $\hat{q}_I$. Note that they imply the relation $\alpha\beta^p - \alpha^p\beta$. Therefore by Theorem 1.1, all relations in $\mathcal{T}_1$ are present. It only remains to prove that κ does not lie in $\mathcal{T}_1$. To see this, note that $\kappa^p = \alpha^{p(p-1)} - \alpha^{(p-1)^2}\beta^{p-1} + \beta^{p(p-1)}$. This is not the p-th power of any polynomial in α and β. ∎

In $\mathcal{Q}_1 \otimes \mathcal{Q}_1$, we need to be able to distinguish the κ of the first factor from that of the second. Write κ', κ'' for $\kappa \otimes 1$, $1 \otimes \kappa$ respectively. Let $\mathcal{T}_{1,1}$ denote the subring $\mathcal{T}_1 \otimes \mathcal{T}_1$ of $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. Both $\mathcal{T}_2$ and $\mathcal{T}_{1,1}$ have generators α_1, α_2, β_1, β_2. In $\mathcal{T}_{1,1}$ however, the relations are generated by $\alpha_1{\beta_1}^p - {\alpha_1}^p\beta_1$ and $\alpha_2{\beta_2}^p - {\alpha_2}^p\beta_2$.

LEMMA 4.2. *Suppose the polynomial $f \in \mathcal{T}_{1,1}[y_1, y_2]$ has no constant term. The coefficients of f belong themselves to a graded ring. $f(\kappa', \kappa'')$ lies in the sub $\mathcal{T}_{1,1}$-module of $\mathcal{Q}_1 \otimes \mathcal{Q}_1$ generated by κ' and κ'' if and only if the coefficients in f of both y_1y_2 and $y_1^2y_2^2$ have no degree zero term.*

Proof. ${\kappa'}^r{\kappa''}^s \in \mathcal{T}_{1,1}$ if and only if neither r nor s is one. Removing, for all such (r, s), both $y_1^{r+1}y_2^s$ and $y_1^r y_2^{s+1}$ from the set of monomials in y_1, y_2, we are left with 1, y_1y_2 and $y_1^2y_2^2$. If δ is one of the generators of $\mathcal{T}_{1,1}$, then $\delta\kappa'\kappa''$ and $\delta{\kappa'}^2{\kappa''}^2$ lie in the submodule in question. So it remains to show that $\kappa'\kappa''$ and its square do not. As $\kappa'\kappa''$ lying there would imply that ${\kappa'}^2{\kappa''}^2$ did too, it is enough to show that ${\kappa'}^2{\kappa''}^2$ is not in the $\mathcal{T}_{1,1}$-module generated by κ' and κ''.

Suppose that ${\kappa'}^2{\kappa''}^2 = g\kappa' + h\kappa''$, with g, $h \in \mathcal{T}_{1,1}$. Since ${\kappa'}^2{\kappa''}^2$ does, $g\kappa' + h\kappa''$ must involve $\alpha_1^{p-1}\alpha_2^{p-1}\beta_1^{p-1}\beta_2^{p-1}$ too. But every term in $g\kappa'$ must involve either α_1^p or β_1^p, and every term in $h\kappa''$ must involve either α_2^p or β_2^p. Since the only relations in $\mathcal{T}_{1,1}$ are $\alpha_1\beta_1^p = \alpha_1^p\beta_1$ and $\alpha_2\beta_2^p = \alpha_2^p\beta_2$, we have derived a contradiction. ∎

LEMMA 4.3. *Suppose that u, $v \in \mathcal{T}_{1,1}$ satisfy $u\kappa' = v\kappa''$. Then $u - v$ lies in the ideal in $\mathcal{T}_{1,1}$ generated by $\alpha_1{\alpha_2}^p - {\alpha_1}^p\alpha_2$, $\alpha_1{\beta_2}^p - {\alpha_1}^p\beta_2$, $\beta_1{\alpha_2}^p - {\beta_1}^p\alpha_2$ and $\beta_1{\beta_2}^p - {\beta_1}^p\beta_2$.*

Proof. Each of the four elements $u-v$ in the statement satisfies the equation $u\kappa' = v\kappa''$, and so lies in the ideal in question. Conversely, define a monomial $\alpha_1^{r_1}\alpha_2^{r_2}\beta_1^{s_1}\beta_2^{s_2}$ to be *admissible* if both $s_1 < p$ unless $r_1 = 0$, and $s_2 < p$ unless $r_2 = 0$. Then the admissible monomials form a basis for the $\mathbb{F}_p$-vector space $\mathcal{T}_{1,1}$. In particular, u and v may be expressed in terms of this basis.

Since $u\kappa' = v\kappa''$ with both u and $v \in \mathcal{T}_{1,1}$, it follows that $u\kappa'$ and $v\kappa''$ lie in $\mathcal{T}_{1,1}$. Hence every admissible monomial in u has either r_1 or s_1 positive, and every admissible monomial in v has either r_2 or s_2 positive. Then $u\kappa'$ is obtained from u as follows: the coefficients remain the same, and each monomial has r_1 increased by $p-1$, unless $r_1 = 0$, in which case s_1 is increased by $p-1$. Similarily, $v\kappa''$ is obtained from v by increasing r_2 or s_2. Since $u\kappa' = v\kappa''$, there is an induced bijection between the admissible monomials in u and in v, and the difference between any admissible monomial in u and the corresponding monomial in v is divisible by one of the four elements in the statement. ∎

LEMMA 4.4. *Let $f \in \mathcal{T}_2[x_0, x_1]$; then, in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$,*

$$\pi^*(\Delta(f)) = f\left(\kappa'\kappa''(\kappa'-\kappa'')^{p-1}, \kappa''(\kappa'-\kappa'')^{p-1} + \kappa'^p\right) - f(0, \kappa'^p) .$$

Moreover, $\pi^*(\gamma_2) = (\kappa' - \kappa'')^p$.

Proof. The maps $\mathcal{Q}_1 \otimes \mathcal{Q}_1 \to S(I^*)$, for all $I \in \Phi$, detect the elements of $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. Using Lemma 3.5 and Eqn. (2), it is straightforward to verify that the equations $\pi^*(\gamma_2) = (\kappa'-\kappa'')^p$, $\pi^*(\kappa_0) = \kappa'\kappa''(\kappa'-\kappa'')^{p-1}$, $\pi^*(\kappa_1) = (\kappa'^{p+1} - \kappa''^{p+1})/(\kappa'-\kappa'')$, $\pi^*(D_0(\alpha_1,\beta_1)) = 0$ and $\pi^*(D_1(\alpha_1,\beta_1)) = \kappa'^p$ hold after mapping to any such $S(I^*)$. ∎

5. DERIVING THE RELATIONS

LEMMA 5.1. *Though κ_1 does not belong to $\mathcal{T}_2$, its p^{th} power does:*

$$\kappa_1^p = \sum_{i=0}^{p} D_1(\alpha_1,\beta_1)^{p-i} D_1(\alpha_2,\beta_2)^i . \tag{4}$$

Proof. Inflate to $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. Now, $\kappa^s \otimes \kappa^t$ belongs to $\mathcal{T}_{1,1}$ if and only if neither s nor t equals 1. Then $\pi^*(\kappa_1)$ equals $\kappa^{p-1} \otimes \kappa + \kappa \otimes \kappa^{p-1}$ modulo $\mathcal{T}_{1,1}$, by Lemma 4.4. So $\kappa_1 \notin \mathcal{T}_2$.

If $I \in \Psi$ then $\hat{q}_I(D_1(\alpha_i,\beta_i)) = D_1(I^*)$ for $i = 1, 2$. Also, $\pi^*(D_1(\alpha_i,\beta_i))$ is κ'^p, κ''^p for $i = 1, 2$ respectively. This establishes Eqn. (4). ∎

We now look at the $\mathcal{T}_2$-submodule of $\mathcal{Q}_2$ generated by 1 and κ_1.

Proposition 5.2. *Let $f \in \mathcal{T}_2[x_0, x_1]$ be a polynomial with coefficients in $\mathcal{T}_2$. The element $f(\kappa_0, \kappa_1)$ of $\mathcal{Q}_2$ belongs to $\mathcal{T}_2\kappa_1 + \mathcal{T}_2$ if and only if the coefficients in f of x_0 and, if $p = 3$, of x_1^2 have no degree zero part.*

Proof. By Proposition 3.3, $f(\kappa_0, \kappa_1)$ belongs to $\mathcal{T}_2\kappa_1 + \mathcal{T}_2$ if and only if there exist $a, b \in \mathcal{T}_2$ such that the equation $\Delta(f) = a\gamma_2 + b\Delta(x_1)$ holds after inflation to $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. Lemma 4.4 says: this is the case if and only if there exist $a', b' \in \mathcal{T}_{1,1}$ such that, in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$,

$$\begin{aligned} & f\left(\kappa'\kappa''(\kappa' - \kappa'')^{p-1}, \kappa''(\kappa' - \kappa'')^{p-1} + \kappa'^p\right) - f(0, \kappa'^p) \\ = \quad & a'(\kappa' - \kappa'')^p + b'\kappa''(\kappa' - \kappa'')^{p-1} . \end{aligned}$$

Note that both sides of the equation are divisible by $(\kappa' - \kappa'')^{p-1}$. Performing this division on the right hand side yields $a'\kappa' + (b' - a')\kappa''$. So by Lemma 4.2, such a', b' exist if and only if the coefficients of both y_1y_2 and $y_1^2y_2^2$ in

$$\frac{f(y_1y_2(y_1 - y_2)^{p-1}, y_2(y_1 - y_2)^{p-1} + y_2^p) - f(0, y_1^p)}{(y_1 - y_2)^{p-1}}$$

have no zero degree term. This happens exactly when the coefficients in $f(x_0, x_1)$ of x_0 and, if $p = 3$, of x_1^2, have no zero degree part. ■

Lemma 5.3. *Let $\delta \in q(E_2^*)$. Then $\delta\kappa_0 = \delta^p\kappa_1 - \delta^{p^2}$.*

Proof. Apply $\hat{q}_I$ for any maximal totally isotropic subspace I. This sends δ to some element of I^*, and κ_r to $D_r(I^*)$. Observe that the left hand side of Eqn. (1) vanishes whenever X is an element of V. ■

Proposition 5.4. $(\delta_1{\delta_2}^p - {\delta_1}^p\delta_2)\,(\kappa_1 - D_1(\delta_1, \delta_2)) = 0$ *for all* $\delta_1, \delta_2 \in E^*$.

Proof. Let I be a maximal totally isotropic subspace of E_2. If $\hat{q}_I(\delta_1)$, $\hat{q}_I(\delta_2)$ are linearly independent in I^*, then κ_1 and $D_1(\delta_1, \delta_2)$ both map to $D_1(I^*)$ under $\hat{q}_I$. If they are linearly dependent, then $\hat{q}_I(\delta_1{\delta_2}^p - {\delta_1}^p\delta_2) = 0$. ■

We can now derive a presentation for the $\mathcal{T}_2$-module generated by 1 and κ_1.

Lemma 5.5. *The ideals J_1,J_2 in $\mathcal{T}_2$ defined as follows are equal.*
J_1 consists of all $u \in \mathcal{T}_2$ with $u\kappa_1 \in \mathcal{T}_2$. Generators of J_2 are $\alpha_1{\alpha_2}^p - {\alpha_1}^p\alpha_2$, $\alpha_1{\beta_2}^p - {\alpha_1}^p\beta_2$, $\beta_1{\alpha_2}^p - {\beta_1}^p\alpha_2$, $\beta_1{\beta_2}^p - {\beta_1}^p\beta_2$ and $\alpha_1{\beta_1}^p - {\alpha_1}^p\beta_1$.

Proof. By Proposition 5.4, $J_2 \subseteq J_1$. We shall show that $J_1 \subseteq J_2$. First we reduce this to a problem in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. Let $u \in J_1$. Then $u\kappa_1 \in \mathcal{T}_2$, so by Proposition 3.3, $u(\kappa_1 - D_1(\alpha_1, \beta_1)) = v\gamma_2$ for some $v \in \mathcal{T}_2$. Now inflate to $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. We get $\pi^*(u)\kappa''(\kappa' - \kappa'')^{p-1} = \pi^*(v)(\kappa' - \kappa'')^p$. Since $(\kappa' - \kappa'')^{p-1}$ is a non-zero divisor in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$, we cancel and rearrange to get $\pi^*(u + v)\kappa'' = \pi^*(v)\kappa'$. By Lemma 4.3, it follows that $\pi^*(u)$ lies in the ideal in $\mathcal{T}_{1,1}$ generated by the images under π^* of the first four generators of J_2. Since the kernel in $\mathcal{T}_2$ of inflation is principal, generated by the fifth generator of J_2, we are done. ■

The following lemma will help us to describe some elements of $\mathcal{T}_2$ involved in relations in $\mathcal{Q}_2$.

LEMMA 5.6. *Suppose that $u \in \mathcal{Q}_2$ satisfies $\hat{q}_I(u) = 0$ for all $I \in \Psi$. Then for each $t \in \mathcal{T}_{1,1}$, there is a unique $v \in \mathcal{Q}_2$ such that $\hat{q}_I(v) = 0$ for all $I \in \Psi$ and $\pi^*(v) = t\pi^*(u)$. It therefore makes sense to refer to v as tu. In particular, this result holds for $u = \gamma_2$, and for $u = \Delta(f)$ for any $f \in \mathcal{T}_2[x_0, x_1]$.*

Proof. The inflation map $\mathcal{T}_2 \to \mathcal{T}_{1,1}$ is surjective. Pick any $\hat{t} \in \mathcal{T}_2$ such that $\pi^*(\hat{t}) = t$. Then $\hat{t}u$ satisfies the requirements on v. The uniqueness part follows from Lemma 3.1 and the definition of $\mathcal{Q}_n$. ∎

We can now put the above results together to obtain a presentation for $\mathcal{Q}_2$. Define polynomials f_1, $f_2 \in \mathbb{F}_p[y_1, y_2]$ to be $y_1^2(y_1^{p+1} - y_2^{p+1})/(y_1^2 - y_2^2)$, respectively $y_1^2 y_2^2(y_1^{p-3} - y_2^{p-3})/(y_1 - y_2) + 2y_1^p + y_1^{p-2}y_2^2 + 2y_2^p$.

THEOREM 5.7. *A presentation for the commutative $\mathbb{F}_p$-algebra $\mathcal{Q}_2$ consists of six generators α_1, α_2, β_1, β_2, κ_0, κ_1, together with relations as follows:*

$$\alpha_1{\beta_1}^p - {\alpha_1}^p\beta_1 + \alpha_2{\beta_2}^p - {\alpha_2}^p\beta_2 = 0 \tag{5}$$

$$\alpha_1{\beta_1}^{p^2} - {\alpha_1}^{p^2}\beta_1 + \alpha_2{\beta_2}^{p^2} - {\alpha_2}^{p^2}\beta_2 = 0 \tag{6}$$

$$(\delta_1{\delta_2}^p - {\delta_1}^p\delta_2)\,(\kappa_1 - D_1(\delta_1, \delta_2)) = 0 \quad \text{for } \delta_1, \delta_2 \in \{\alpha_1, \beta_1, \alpha_2, \beta_2\} \tag{7}$$

$$\delta\kappa_0 - \delta^p\kappa_1 + \delta^{p^2} = 0 \quad \text{for } \delta \in \{\alpha_1, \beta_1, \alpha_2, \beta_2\} \tag{8}$$

$$\kappa_1^p = \sum_{i=0}^{p} D_1(\alpha_1, \beta_1)^{p-i} D_1(\alpha_2, \beta_2)^i \tag{9}$$

$$\Delta(x_0^2) = \kappa'^2\kappa''^2(\kappa' - \kappa'')^{p-2}\gamma_2 \tag{10}$$

$$\Delta(x_0x_1) = (f_1(\kappa', \kappa'') + f_1(\kappa'', \kappa'))\,\Delta(x_1) + f_1(\kappa'', \kappa')\gamma_2\ . \tag{11}$$

If $p > 3$ then

$$\Delta(x_1^2) = f_2(\kappa', \kappa'')\Delta(x_1) + (\kappa'^{p-2}\kappa''^2 + \kappa''^p)\gamma_2 \tag{12}$$

If $p = 3$, then Eqn. (12) is replaced by the relations

$$\Delta(\varepsilon_1 x_1^2) = (\varepsilon_1\kappa''^3 + 2\varepsilon_1^3\kappa''^2 + 2\varepsilon_1^7)\Delta(x_1) + \varepsilon_1^3\kappa''^2\gamma_2 \quad \text{for } \varepsilon_1 = \alpha_1, \beta_1 \tag{13}$$

$$\Delta(\varepsilon_2 x_1^2) = (2\varepsilon_2\kappa'^3 + \varepsilon_2^3\kappa'^2 + 2\varepsilon_2^7)\Delta(x_1) + \varepsilon_2^7\gamma_2 \quad \text{for } \varepsilon_2 = \alpha_2, \beta_2. \tag{14}$$

In fact, Eqn. (9) is a consequence of the other relations if $p > 3$, though this would be hard to verify directly. Note that Eqn. (6) is redundant too: this can be seen from above.

The only relations in $\mathcal{T}_2$ are the first two relations above; the first three relations above carry all information about $\mathcal{T}_2\kappa_1 + \mathcal{T}_2$.

Proof. It only remains to establish the last five relations. All are proved using the method of the proof of Proposition 5.2. We give one example, the case of $\Delta(x_0x_1)$. We have

$$\pi^*(\Delta(x_0x_1)) = \kappa'\kappa''(\kappa'-\kappa'')^{p-1}(\kappa'^{p+1}-\kappa''^{p+1})/(\kappa'-\kappa'') \; ,$$

and require $a', b' \in \mathcal{T}_{1,1}$ such that

$$\begin{aligned} a'\kappa' + (b'-a')\kappa'' &= (\kappa'^{p+2}\kappa'' - \kappa'\kappa''^{p+2})/(\kappa'-\kappa'') \\ &= (\kappa'^{p+3}\kappa'' - \kappa'^2\kappa''^{p+2} - \kappa'\kappa''^{p+3} + \kappa'^{p+2}\kappa'')/(\kappa'^2-\kappa''^2) \\ &= f_1(\kappa'',\kappa')\kappa' + f_1(\kappa',\kappa'')\kappa'' \; . \end{aligned}$$

As both $f_1(\kappa'',\kappa')$ and $f_1(\kappa',\kappa'')$ lie in $\mathcal{T}_{1,1}$, we are done. ■

6. EXTRASPECIAL p-GROUPS

The $2n$-dimensional $\mathbb{F}_p$-vector space E_n may be viewed as an elementary abelian p-group of rank $2n$. Let N be a cyclic group of order p. The nondegenerate symplectic form b on E may be viewed as a map $E \times E \to N$. Denote by P_n the extraspecial p-group p_+^{1+2n} of order p^{2n+1} and exponent p. There is a central extension $1 \to N \to P_n \xrightarrow{\psi} E \to 1$, such that, for $g_1, g_2 \in P_n$, the commutator $[g_1, g_2]$ equals $b\,(\psi(g_1), \psi(g_2))$. The maximal elementary abelian subgroups of P_n have p-rank $n+1$, and are exactly the inverse images under ψ of the maximal totally isotropic subspaces of E.

To determine the irreducible characters of P_n, pick an embedding of the additive group of $\mathbb{F}_p$ in $\mathbb{C}^\times$. There are p^{2n} linear characters of P_n, all of which factor through ψ. These may be identified with the elements of the dual space E_n^*. The $p-1$ remaining irreducible characters all have degree p^n and are induced from any maximal elementary abelian subgroup of P_n. Let $\hat{\chi}$ be a nontrivial linear character of N. Then for each $1 \leqslant i \leqslant p-1$ there is an irreducible character χ_i of P_n whose restriction to any maximal elementary abelian subgroup M is the sum of all linear characters of M whose restriction to N is $\hat{\chi}^{\otimes i}$.

For each $\phi \in E_n^*$, pick a representation ρ_ϕ of P_n whose character is linear, corresponding to ϕ. Let ρ_1 be a representation of P_n affording the character χ_1.

Definition 6.1. For any finite group G, define $h^*(G)$ to be the quotient of the graded commutative ring $\mathrm{H}^*(G,\mathbb{F}_p)$ by its nilradical. Define $ch(G)$ to be the subring of $h^*(G)$ generated by the images under the homomorphism $\mathrm{H}^*(G,\mathbb{Z}) \to \mathrm{H}^*(G,\mathbb{F}_p) \to h^*(G)$ of the Chern classes of the representations of G.

The reader is referred to the appendix of Atiyah's paper [**1**] for a concise introduction to Chern classes of group representations. A proof of the following theorem may be found in Chapter 8 of Evens' book [**4**].

THEOREM 6.2. (Quillen) *Let G be a finite group, and let ξ be a class in $h^*(G)$. Then ξ is zero if and only if $\mathrm{Res}_E\,\xi = 0$ in $h^*(E)$ for every elementary abelian p-subgroup E of G.* ∎

Recall that $\mathcal{Q}_n$ is defined in terms of the polynomial algebra $S(E_n^*) \otimes_{\mathbb{F}_p} \mathbb{F}_p[K_0, \ldots, K_{n-1}]$, denoted F_n.

THEOREM 6.3. *Let Z be an indeterminate. There is a unique $\mathbb{F}_p$-algebra homomorphism $f\colon F_n \otimes_{\mathbb{F}_p} \mathbb{F}_p[Z] \to \mathrm{H}^*(p_+^{1+2n}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_p$ which sends $\phi \in E_n^*$ to $c_1(\rho_\phi)$, sends K_r to $(-1)^{n-r} c_{p^n - p^r}(\rho_1)$, and sends Z to $c_{p^n}(\rho_1)$. This homomorphism induces an isomorphism $\bar{f}\colon \mathcal{Q}_n \otimes_{\mathbb{F}_p} \mathbb{F}_p[Z] \to ch(p_+^{1+2n})$.*

Proof. Let ρ, σ be degree one representations of P_n. Since $c_1(\rho \otimes \sigma) = c_1(\rho) + c_1(\sigma)$, the algebra homomorphism f is well-defined; clearly it is unique.

Any elementary abelian p-group A may be viewed as an $\mathbb{F}_p$-vector space. There is an isomorphism $ch(A) \to S(A^*)$ which sends the first Chern class of any degree one representation to the corresponding element of A^*. Moreover, $ch(A) = h^*(A)$.

For $1 \leqslant j \leqslant p-1$, let ρ_j be a representation of P_n which affords the character χ_j. Let I be any maximal totally isotropic subspace of E_n, and let M be the corresponding maximal elementary abelian subgroup of P_n. Then I^* is the subspace of M^* which annihilates N. Pick some $\gamma \in h^2(M)$ such that $\mathrm{Res}_N(\gamma) = c_1(\hat{\chi})$. If we restrict the total Chern class of ρ_j to M and apply the Whitney sum formula, we have

$$\begin{aligned} \mathrm{Res}_M\, c(\rho_j) &= \prod_{v \in I^*} (1 + v + j\gamma)\,, \\ &= 1 + \sum_{r=0}^{n-1} (-1)^{n-r} D_r(I^*) + j\left(\gamma^{p^n} + \sum_{r=0}^{n-1} (-1)^{n-r} D_r(I^*)\gamma^{p^r}\right)\,. \end{aligned}$$

By Quillen's Theorem, $c_{p^n-p^r}(\rho_j) = c_{p^n-p^r}(\rho_1)$ and $c_{p^n}(\rho_j) = j c_{p^n}(\rho_1)$ in $ch(P_n)$. Moreover, these are the only non-zero Chern classes of the induced representations. Hence the map from $\mathrm{H}^*(P_n, \mathbb{Z}) \otimes \mathbb{F}_p$ down to $h^*(G)$ maps $\mathrm{Im}(f)$ onto $ch(P_n)$. Observe that Z is the only generator of $F_n \otimes \mathbb{F}_p[Z]$ whose image under $\mathrm{Res}_M \circ f$ involves γ, and that $\mathrm{Res}_M\, f(Z)$ is transcendental over $S(I^*)$. Therefore, we only have to show that the induced map $\mathcal{Q}_n \to ch(P_n)$ is both injective and well-defined. But, for every $y \in F_n$ and for every I, the elements $q_I(y)$ and $\mathrm{Res}_M\, f(y)$ of $S(I^*)$ are equal. The result then follows by Quillen's Theorem and the definition of $\mathcal{Q}_n$. ∎

REMARK. Both f and $\bar{f}$ double the degree of homogeneous elements.

REMARK. There is one other extraspecial p-group of order p^5, and it has exponent p^2. The same methods may be used to investigate its mod-p cohomology ring and to determine a presentation for the Chern subring modulo nilradical. Both the calculation and the result are simpler: in fact, one of the first Chern classes is a non-zero divisor. It is because there are fewer maximal elementary abelian subgroups and a smaller automorphism group that this calculation is easier. But the group is less interesting, for the same reasons.

7. A GENERAL INEQUALITY

It is the business of this section to prove that $\mathcal{Q}_n$ always strictly contains $\mathcal{T}_n$. Specifically, we prove the following theorem.

THEOREM 7.1. *For every $n \geqslant 1$, we have $\kappa_{n,0} \notin \mathcal{T}_n$. Hence $c_{p^n-1}(\rho_1)$ lies outside the subring of $\mathrm{ch}(P_n)$ generated by the first Chern classes and $c_{p^n}(\rho_1)$.*

Proof. Proposition 4.1 gives us the case $n = 1$. We shall prove the rest of the result by considering the inflation map $\pi^*\colon \mathcal{Q}_{n+1} \to \mathcal{Q}_1 \otimes_{\mathbb{F}_p} \mathcal{Q}_n$, and showing that $\pi^*(\kappa_{n+1,0})$ lies outside $\mathcal{T}_1 \otimes \mathcal{Q}_n$ for all $n \geqslant 1$.

The inflation map is associated to the orthogonal direct sum decomposition $E_{n+1} = E_1 \perp E_n$. For each maximal elementary abelian subgroup I_{n+1} of E_{n+1} this induces the decomposition $I_{n+1} = I_1 \oplus I_n$. Using this decomposition and Eqn. (1), we can express the Dickson invariants of I_{n+1} in terms of the Dickson invariants for I_1 and I_n. In particular, if we define $D_n(I_n) = 1$, then

$$D_0(I_{n+1}^*) = (D_0(I_1^*) \otimes D_0(I_n^*)) \left(\sum_{j=0}^{n} (-1)^j D_0(I_1^*)^{\frac{p^{n-j}-1}{p-1}} \otimes D_{n-j}(I_n^*) \right)^{p-1} ,$$

whence, also defining $\kappa_{n,n} = 1$, we have

$$\pi^*(\kappa_{n+1,0}) = (\kappa \otimes \kappa_{n,0}) \left(\sum_{j=0}^{n} (-1)^j \kappa^{\frac{p^{n-j}-1}{p-1}} \otimes \kappa_{n,n-j} \right)^{p-1} . \tag{15}$$

Since $\kappa^r \in \mathcal{T}_1$ if and only if $r \neq 1$, the right hand side of this equation equals $\kappa \otimes \kappa_{n,0}^p$ modulo $\mathcal{T}_1 \otimes \mathcal{Q}_n$. ∎

8. SYMPLECTIC INVARIANTS

Closely related to the work of this paper is a question about symplectic invariants. The symplectic group $Sp_{2n}(\mathbb{F}_p)$ is by definition the group of those linear transformations of E_n which preserve the nondegenerate symplectic form b. The invariants of the action of $Sp_{2n}(\mathbb{F}_p)$ on $S(E_n^*)$ were determined by Carlisle and Kropholler, and are described in Section 8.3 of Benson's book [**2**].

The ring of invariants in $S(E_n^*)$ is generated by $R_1(E_n^*)$, ..., $R_{2n-1}(E_n^*)$, $D_n(E_n^*)$, ..., $D_{2n-1}(E_n^*)$. Recall from Theorem 1.1 that the quotient of $S(E_n^*)$ by the ideal generated by the regular sequence $R_1(E_n^*)$, ..., $R_n(E_n^*)$ is $\mathcal{T}_n$. There is therefore an induced action of $Sp_{2n}(\mathbb{F}_p)$ on $\mathcal{T}_n$. It is natural to ask what is the ring of invariants of this action.

By the Tezuka–Yagita Theorem, every $R_r(E_n^*)$ is zero in $\mathcal{T}_n$. Certainly every $D_r(E_n^*)$ is still invariant. But now there are other invariants as well.

Proposition 8.1. *The natural action of $Sp_{2n}(\mathbb{F}_p)$ on $\mathcal{T}_n$ has as ring of invariants the intersection of $\mathcal{T}_n$ with $\mathbb{F}_p[\kappa_{n,0},\ldots,\kappa_{n,n-1}]$.*

Proof. The symplectic group permutes the maximal totally isotropic subspaces I of E_n transitively. In addition, for any I, every automorphism of I may be extended to a symplectic transformation on E_n. Hence, for every I and for every symplectic invariant $x \in \mathcal{T}_n$, the element $\hat{q}_I(x)$ of $S(I^*)$ is invariant under $GL(I)$, and this invariant is independent of I. Since the Dickson invariants in $S(I^*)$ generate the invariants under $GL(I)$, it follows that x equals some polynomial over $\mathbb{F}_p$ in $\kappa_{n,0}$, ..., $\kappa_{n,n-1}$. Conversely, any such polynomial is invariant under the action of $Sp_{2n}(\mathbb{F}_p)$ on $\mathcal{Q}_n$. ∎

Theorem 8.2. *The ring of invariants under the natural action of $Sp_4(\mathbb{F}_p)$ on $\mathcal{T}_2$ is the subring of the polynomial algebra $\mathbb{F}_p[\kappa_0,\kappa_1]$ of polynomials whose support contains neither any $\kappa_0\kappa_1^r$ with $r \geqslant 0$ nor any κ_1^r with $p \nmid r$. Over the polynomial algebra $\mathbb{F}_p[\kappa_0^2,\kappa_1^p]$, the ring of invariants is the free module generated by 1, $\kappa_0^2\kappa_1^s$ for $1 \leqslant s \leqslant p-1$, and $\kappa_0^3\kappa_1^s$ for $0 \leqslant s \leqslant p-1$.*

Proof. Let $f(x_0,x_1)$ be any polynomial in $\mathbb{F}_p[x_0,x_1]$. By Proposition 3.3, $f(\kappa_0,\kappa_1)$ belongs to $\mathcal{T}_2$ if and only if there exists $a \in \mathcal{T}_2$ such that

$$f(\kappa_0,\kappa_1) - f\left(D_0(\alpha_1,\beta_1), D_1(\alpha_1,\beta_1)\right) = a\gamma_2$$

holds after inflation to $\mathcal{Q}_1 \otimes \mathcal{Q}_1$. That is, if and only if there exists $a' \in \mathcal{T}_{1,1}$ such that, in $\mathcal{Q}_1 \otimes \mathcal{Q}_1$,

$$f\left(\kappa'\kappa''(\kappa'-\kappa'')^{p-1}, \kappa''(\kappa'-\kappa'')^{p-1} + \kappa'^p\right) - f(0,\kappa'^p) = a'(\kappa'-\kappa'')^p\,. \quad (16)$$

Both sides of Eqn. (16) are divisible by $(\kappa'-\kappa'')^{p-1}$. Doing this to the right hand side yields $a'(\kappa'-\kappa'')$. Suppose f is the monomial $x_0^r x_1^s$. If $r \geqslant 2$, then $f(\kappa_0,\kappa_1) \in \mathcal{T}_2$. If $r = 1$, then the left hand side of Eqn. (16) is $\kappa'\kappa''(\kappa' - \kappa'')^{p-1}\left(\kappa''(\kappa'-\kappa'')^{p-1} + \kappa'^p\right)^s$, not divisible by $(\kappa'-\kappa'')^p$. If $r = 0$, then it is

$(\kappa''(\kappa'-\kappa'')^{p-1}+\kappa'^p)^s-\kappa'^{sp}$, divisible by $(\kappa'-\kappa'')^p$ if and only if $p \mid s$. The monomials $x_0^r x_1^s$ such that $\kappa_0^r\kappa_1^s \notin \mathcal{T}_2$ all have distinct degrees when evaluated at (κ_0,κ_1). Hence $\mathbb{F}_p[\kappa_0,\kappa_1]\cap\mathcal{T}_2$ is the subring of $\mathbb{F}_p[\kappa_0,\kappa_1]$ described in the statement. Now use Proposition 8.1. ∎

REMARK. Using Theorem 5.7, we could in principle give expressions in terms of the α_i and β_j for each generator of this ring of invariants: however, these expressions would be very complicated. The current form of the result is likely to be the more illuminating.

ACKNOWLEDGEMENTS

The support of the Max Kade Foundation is gratefully acknowledged, as is the kind hospitality of the University of Chicago.

The author wishes to thank J. L. Alperin and I. J. Leary for encouragement and helpful conversations.

REFERENCES

[**1**] M. F. Atiyah. Characters and cohomology of finite groups. *Inst. Hautes Études Sci. Publ. Math.* **9** (1961), 23–64.

[**2**] D. J. Benson. *Polynomial Invariants of Finite Groups.* London Math. Soc. Lecture Note Ser. no. 190 (Cambridge Univ. Press, 1993).

[**3**] D. J. Benson and J. F. Carlson. The cohomology of extraspecial groups. *Bull. London Math. Soc.* **24** (1992), 209–235. Erratum: *Bull. London Math. Soc.* **25** (1993), 498.

[**4**] L. Evens. *The Cohomology of Groups.* (Oxford Univ. Press, 1991).

[**5**] D. J. Green and I. J. Leary. Chern classes and extraspecial groups. *Manuscripta Math.* **88** (1995), 73–84.

[**6**] I. J. Leary. The mod-p cohomology rings of some p-groups. *Math. Proc. Cambridge Philos. Soc.* **112** (1992), 63–75.

[**7**] G. Lewis. The integral cohomology rings of groups of order p^3. *Trans. Amer. Math. Soc.* **132** (1968), 501–529.

[**8**] D. Quillen. The mod 2 cohomology rings of extra-special 2-groups and the spinor groups. *Math. Ann.* **194** (1971), 197–212.

[**9**] M. Tezuka and N. Yagita. The varieties of the mod p cohomology rings of extra special p-groups for an odd prime p. *Math. Proc. Cambridge Philos. Soc.* **94** (1983), 449–459.