Rings of invariants of modular $p$-groups
which are hypersurfaces

I.P. Hughes $^{a,*}$, N. Kechagias $^b$

$^a$ Department of Mathematics and Statistics, Queen’s University, Kingston, ON, K7L 3N6, Canada
$^b$ Department of Mathematics, University of Ioannina, Ioannina 45110, Greece

Received 22 January 2004
Available online 21 July 2005
Communicated by Peter Littelmann

Abstract

For $L$ a finite non-modular group whose invariants form a polynomial ring and $H$ a subgroup of $L$ containing the derived group of $L$, Nakajima found necessary and sufficient conditions on $H$ for its invariant ring $S^H$ to be a hypersurface. In a crucial step of his proof he showed that if $S^H$ is a hypersurface, then between $H$ and $L$ there is a group $G$ with polynomial invariant ring such that $S^H = S^G[h]$.

For $G$ a finite modular $p$-group over $F_p$ with polynomial invariant ring and $H$ a subgroup of $G$ containing the derived group of $G$, we find necessary and sufficient conditions on $H$ to ensure that $S^H = S^G[h]$.

$^*$ Corresponding author.

$^*$ E-mail addresses: hughesi@mast.queensu.ca (I.P. Hughes), nkechag@cc.uoi.gr (N. Kechagias).

$^1$ The author is supported by an NSERC grant.

$^2$ 0021-8693/ - see front matter $^c$ 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2005.05.026

1. Introduction

For $V$ an $n$-dimensional vector space over a field $F$, we denote by $S = S(V)$ the symmetric algebra of $V$. The action of the general linear group $GL(V)$ extends naturally to that of a group of degree-preserving automorphisms of $S$. For $G$ a subgroup of $GL(V)$ we
denote by $S^G$ the set of fixed points of $G$ in $S$. If $G$ is finite, then its ring of invariants $S^G$ is a finitely generated graded $F$-subalgebra of $S$ and is the object of study of the invariant theory of finite groups.

Much work has been done on relating the algebraic structure of $S^G$ to properties of $G$ as a finite linear group. Perhaps the most celebrated result in this vein is that of Serre [7] (see [1, p. 85], (ii) $\Rightarrow$ (i) for a proof), namely that if $S^G$ is a polynomial algebra (equivalent to being generated by $n$ elements), then $G$ is a reflection subgroup. By a reflection we mean an element $g$ of $GL(V)$ such that $\dim(g - 1)V = 1$. The converse of Serre’s theorem is true for $G$ a non-modular group, that is, if the characteristic of $F$ does not divide the order of $G$ (for a proof see [3, Theorem, p. 191], or [1, Theorem 7.2.1, p. 83]). However, for $G$ a modular group this converse is false. In fact, there are modular $p$-groups $G$ generated by reflections for which $S^G$ is not even Cohen–Macaulay, whereas $S^G$ is Cohen–Macaulay for all non-modular groups. However, for $F = F_p$ the field of $p$ elements and $G$ a $p$-group, Nakajima [4, Theorem 4.8] found necessary and sufficient conditions on $G$ for $S^G$ to be a polynomial algebra.

Perhaps the closest condition on $S^G$ to being a polynomial algebra is that of being a hypersurface, that is, an algebra with exactly one relation on a minimal generating set. This is equivalent to $S^G$ being generated by $n + 1$ elements.

For $H$ a non-modular subgroup of $GL(V)$, Nakajima [5, Theorem 4.2] found necessary and sufficient condition on $H$ for $S^H$ to be a hypersurface under the assumption that there is a group $L \leq GL(V)$ with polynomial invariant ring such that $[L, L] \leq H \leq L$. A crucial step in the proof is the result [5, Theorem 3.1] that there is a group $G$ between $H$ and $L$ with polynomial invariant ring such that $S^H = S^G[b]$ for some $b$ in $S^H$. The exact analogue of this result is false for $H$ a modular group.

In this article we assume that $G$ is a finite linear $p$-group over $F_p$ with invariants $S^G$ a polynomial ring. We suppose that $H$ is a subgroup of $G$ containing the derived group $[G, G]$. Our main result is Theorem 11 where we find necessary and sufficient conditions on $H$ to ensure that $S^H = S^G[b]$. In the proof we use the result of Campbell–Hughes [2, Theorem 4.4] which states that if $H$ is of index $p$ in $G$ (and so contains $[G, G]$) then $S^H = S^G[b]$. Indeed, our result can be thought of as a generalization of this.

2. Nakajima $p$-groups

Throughout the rest of this paper, $V$ is an $n$-dimensional vector space over $F_p$ and $S = S(V)$ its symmetric algebra. We denote by $S^G$ the invariant algebra of $G$ in $S$, where $G$ is a (necessarily finite) subgroup of $GL(V)$.

We now suppose that $G$ is a $p$-subgroup of $GL(V)$. Then there is at least one basis of $V$ for which $G$ is upper triangular. We assume that $\beta = \{x_1, \ldots, x_n\}$ is one such basis. For $1 \leq i \leq n$ we let

$$G_i := \{g \in G \mid g(x_j) = x_j, \forall j \neq i\}.$$  

Each $G_i$ is an elementary abelian $p$-group each of whose non-identity elements $g$ is a reflection, that is, $\dim_{F_p}(g - 1)V = 1$.  

We shall often use the fact that \( G_j \) normalizes \( G_i \) for \( j < i \). It follows that \( \tilde{G} := G_1 G_2 \cdots G_n \) is a subgroup of \( G \) of order \( \prod_{i=1}^n |G_i| \).

**Definition 1.** We say that \( G \) is a \( \beta \)-Nakajima \( p \)-group if \( G = \tilde{G} \) or equivalently, \( |G| = \prod_{i=1}^n |G_i| \).

The celebrated result of Nakajima [4, Theorem 4.8] mentioned in our induction states that for \( V \) a finite-dimensional vector space over \( F_p \) and \( G \) a \( p \)-subgroup of \( GL(V) \), \( S^G \) is a polynomial algebra if and only if \( G \) is a \( \beta \)-Nakajima \( p \)-group for some basis \( \beta \) of \( V \). We state the “if” part of this theorem giving the generators of \( S^G \) explicitly.

**Lemma 2** [4, Proposition 4.1]. Suppose \( G \) is upper-triangular for a basis \( \beta = \{x_1, \ldots, x_n\} \) of \( V \). Then \( G \) is a \( \beta \)-Nakajima \( p \)-group \( \iff S^G = F[N^{G_i}_i(x_i) \mid 1 \leq i \leq n] \), where \( N^{G_i}_i(x_i) := \prod_{j \in G_i} g_i(x_i) \) is the norm of \( x_i \) under \( G_i \).

We remark in passing that in this theorem \( F_p \) cannot be replaced by an arbitrary field of characteristic \( p \). Indeed, Stong found a \( p \)-subgroup of \( GL(V) \) with polynomial invariants, but which is not a \( \beta \)-Nakajima \( p \)-group for any basis \( \beta \) of \( V \) (see [8]). In Stong’s example \( F \) has \( p^3 \) elements.

**Lemma 3.** Suppose that \( H \) is a subgroup of the \( \beta \)-Nakajima \( p \)-group \( G \). Then

\[
\begin{align*}
(A) & \quad H \triangleleft G \Rightarrow \tilde{H} \triangleleft \tilde{G}; \\
(B) & \quad [G, G] \leq H \Rightarrow [G, G] \leq \tilde{H}, \text{ where } [G, G] \text{ is the commutator subgroup of } G.
\end{align*}
\]

**Proof.** We note that \( G_i \cap H = H_i \) for all \( i \).

(A) Since \( \{G_j \mid 1 \leq j \leq n\} \) (respectively \( \{H_i \mid 1 \leq i \leq n\} \)) generates \( G \) (respectively \( \tilde{H} \)) it is sufficient to prove that \( g_j^{-1} h_j g_j \in \tilde{H} \) for all \( g_j \in G_j \) and \( h_j \in H_j \).

If \( j < i \), since \( G_i \) normalizes \( G_j \) and \( H \triangleleft G \) then \( g_j^{-1} h_j g_j \in G_i \cap H = H_i \subseteq \tilde{H} \).

If \( j \geq i \) then similarly \( [h_i, g_j] := (h_j^{-1} g_j^{-1} h_j) = h_j^{-1} (g_j^{-1} h_j g_j) \in G_j \cap H = H_j \).

Thus \( g_j^{-1} h_j g_j \in H_j \) \( \subseteq \tilde{H} \).

(B) By the identity \([a, c] = [c, ab]^{-1} = (b^{-1} a c b)^{-1} \), since \( \tilde{H} \triangleleft G \) by (A) just proved, it is sufficient to prove that \( g_j, g_j \in \tilde{H} \) for all \( g_j \in G_j \) and \( g_j \in G_j \). Since \([g_j, g_j] = [g_j, g_j]^{-1} \) we may assume that \( j \leq i \). Now \( g_i, g_j = g_j^{-1} (g_j^{-1} g_i g_j) \in H_i \cap G_i = H_i \subseteq \tilde{H} \) since \( [G, G] \subseteq H \) and \( G_j \) normalizes \( G_i \). \( \square \)

3. When \( S^H = S^G[b] \)

The main result in this paper is Theorem 11 (see Section 5) which gives necessary and sufficient conditions on \( H \) for \( S^H \) to be equal to \( S^G[b] \), where \([G, G] \leq H < G \) and \( G \) is a Nakajima \( p \)-group. In this section we obtain consequences of the assumption that \( S^H = S^G[b] \) (Proposition 6). We need
Lemma 4. Let $G \leq GL(V)$. Suppose $y \in S$ and $\{1, y, y^2, \ldots, y^{p-1}\}$ is independent over $S^G$. Let $b = \sum_{i=0}^{r<p} b_i y^i$ such that $b_i \neq 0$ and $b_i \in S^G$ for all $i$. Assume that there is a $g \in G$ satisfying $0 \neq (g - 1)y \in S^G$. Then

(A) $(g - 1)b = 0$ implies $r = 0$ and so $b \in S^G$;
(B) $(g - 1)b \in S^G$ implies $r \leq 1$.

Proof. By direct computation:

$$(g - 1)b = \sum_{i=0}^{r<p} b_i ((y + (g - 1)y)^i - y^i)$$

$$= rb_r ((g - 1)y)^{r-1} + c_{r-2}y^{r-2} + \cdots + c_1 y + c_0$$

uniquely, where $c_i \in S^G$. Since $\{1, y, \ldots, y^{p-1}\}$ is independent over $S^G$, (A) and (B) follow. \qed

We denote by $Q(R)$ the quotient field of the domain $R$.

Lemma 5. Suppose $b \in S$ and $G \leq GL(V)$. If $H := \text{Stab}_G(b)$, the stabilizer of $b$ in $G$, then

(A) $Q(S^G[b]) = Q(S^H)$;
(B) $\{b^i \mid 0 \leq i < [G : H]\}$ is a basis for $S^G[b]$ over $S^G$.

Proof. (A) By Galois theory there is a subgroup $L$ of $G$ containing $H$ such that

$$Q(S^L) = Q(S^G[b]) \quad (\leq Q(S^H)).$$

By this equality $L$ fixes $b$ and so $L \leq H$. However by the above $Q(S^L) \leq Q(S^H)$ and so $H \leq L$. Thus $L = H$ and (A) follows.

(B) Since $b$ is integral over $S^G$ and $S^G$ is integrally closed, it follows by Gauss’ lemma [6, (1.13), p. 5] that the minimal polynomial $m(x)$ of $b$ over $Q(S^G)$ has coefficients in $S^G$. Since $S^H$ is integral over $S^G$, by (A), $Q(S^H) = Q(S^G)[b]$ and the degree of $m(x)$ is $[G : H]$. (B) follows. \qed

For $H \leq L \leq GL(V)$ and $b \in S^H$ we denote the relative norm $\prod_{\ell \in \mathcal{L}} \ell(b)$ by $N^L_H(b)$, where $\mathcal{L}$ is a left transversal of $H$ in $L$. It is independent of the particular left transversal used.

We shall often use the formal identity

$$(gg' - 1) = (g - 1) + (g' - 1) + (g - 1)(g' - 1). \quad (1)$$

Proposition 6. Let $H$ be a normal subgroup of the $p$-group $G \leq GL(V)$. Suppose $S^H = S^G[b]$ for some homogeneous $b \in S^H$. Then
in $SH(B)$ for all $g \in G$. Since $g$ has order $p^r$ for some $r$, it follows that $\alpha = 1$, so $(g - 1)b$ is in $SG$.

(ii) Using (1) and (A)(i) we see that the map $\varepsilon(g) = (g - 1)b$ is a homomorphism and so $[G, G] \subseteq \ker(\varepsilon) = Stab_G(b)$ which is $H$ by Lemma 5(A) since by hypothesis $S^G[b] = SH$.

(B) We proceed by induction on $r$ where $p^r = [L : H]$. We first assume that $r = 1. Since clearly $H = Stab_G(b)$, by Lemma 5(B) any element in $S^H = SG[b]$, and so in particular in $SG$, can be written as a polynomial in $b$ over $SG$ (of degree $< [G : H]$) uniquely. We assume that $S^L \neq S^G[N^L_H(b)]$ and get a contradiction. We suppose $L = \langle g, H \rangle$. We let $s \in S^L \setminus S^G[N^L_H(b)]$ have smallest degree in $b$ over $SG$. Now

$$N^L_H(b) = \prod_{a \in F_p} (b + (g^a - 1)b)$$

and so is a monic polynomial in $b$ over $SG$ by A(i), of degree $p$. So by division: $s = N^L_H(b)q + r$, where $\deg_b q < \deg_b s$ and $\deg_b r \leq p - 1$. Here $q, r \in S^G[b] = SH$. Since $s \in S^L$, we have that $0 = (g - 1)s = N^L_H(b)(g - 1)q + (g - 1)r$ which implies that $(g - 1)q = 0 = (g - 1)r$ and hence $q$ and $r$ are in $S^L$. By the minimality of the degree of $s$ in $b, q \in S^G[N^L_H(b)]$. Now $r = \sum_{i=0}^{p-1} r_i b^i$, where $r_i \in SG$. Since $(g - 1)r = 0$, by Lemma 4(A), we get $r \in S^G$. Thus $s \in S^G[N^L_H(b)]$, a contradiction. We conclude that $S^L = S^G[N^L_H(b)]$.

We now assume that $r > 1$. We pick $K$ such that $H < K < L$ with $[K : H] = p$. By the case $r = 1$ we have $S^K = S^G[N^K_H(b)]$. Since $[G : G] \leq H$ by (A)(ii), $K$ is normal in $G$. So we can apply the inductive hypothesis to conclude that $S^L = S^G[N^K_H(b)] = S^G[N^L_H(b)]$. \[\square\]

4. An expression for special elements of $SH$

In the proof of our main result (Theorem 11) we define an element $b$ in $S^H$ and ultimately show that $S^H = S^G[b]$. In Proposition 8 below we obtain an expression for any $b$ in $S^H$ which satisfies Proposition 6(A)(i), namely that $(g - 1)b$ is in $SG$ for all $g \in G$.

But we first introduce certain so-called $p$-polynomials which we use in the proof of Lemma 7 and repeatedly in Section 5.

For a $k$-dimensional vector space $W$ over $F_p$, we define $f_W(X)$ in $S(W)[X]$ as

$$f_W(X) := \prod_{w \in W} (X + w), \quad (2)$$
where $S(W)$ is the symmetric algebra of $W$. By induction on $k$, 
$$f_W(X) = X^{p^k} + a_{k-1}X^{p^{k-1}} + \cdots + a_0X,$$
where $a_i \in S(W), 0 \leq i \leq k-1$. It is then clear that

$$f_W(X + Y) = f_W(X) + f_W(Y).$$

The polynomial $f_W(X)$ is an example of a $p$-polynomial.

We assume throughout this section that $\beta = \{x_1, \ldots, x_n\}$ is a fixed basis of $V$ and $H$ is a subgroup of the $\beta$-Nakajima $p$-group $G$. So by Definition 1, $G = G_1G_2 \cdots G_n$.

Now $(hi - 1)x_i \in \langle x_1, \ldots, x_{i-1}\rangle_{F_p}$ for all $hi \in H_i = H \cap G_i$. So using (1) it is clear that $V(H_i) := \{(hi - 1)x_i | hi \in H_i\}$ is a subspace of $V$. Let

$$y_i := N_{H_i}(x_i) = \prod_{hi \in H_i} hi(x_i) = f_V(H_i)(x_i).$$

(4)

Since for $hi, h'_i \in H_i$ we have $(hi - 1)x_i = (h'_i - 1)x_i$ only if $hi = h'_i$. It follows from (3) and using (1) that

$$(gi - 1)y_i = \prod_{hi \in H_i} (gihi - 1)x_i.$$  

(5)

Lemma 7. Let $H \leq G$, where $G$ is a $\beta$-Nakajima $p$-groups.

(A) If $H \triangleleft G$ then for $j \neq i$ each element of $G_j$ fixes $y_i$.
(B) $[G, G] \leq H \iff (g - 1)y_i \in S^G$ for all $g \in G$.

Proof. (A) Let $g_j \in G_j$. If $j > i$ then $g_jhi(x_i) = hi(x_i)$ for all $h_i \in H_i$ since $h_i(x_i) \in \langle x_1, \ldots, x_{i-1}\rangle_{F_p}$ and so

$$g_jy_i = g_j \prod_{h_i \in H_i} hi(x_i) = y_i.$$  

If $j < i$ then

$$g_jy_i = \prod_{h_i \in H_i} g_jhi_{h_j}^{-1}(x_i) = y_i$$

since $g_j$ normalizes both $H$ and $G_i$ and so also $H_i = H \cap G_i$.

(B) We assume $[G, G] \leq H$. We first show that $(gi - 1)y_i \in S^G$, for all $gi \in G_i$. We let $g_i \in G_i$. Since $G$ is generated by $\{g_j | 1 \leq j \leq n\}$ we need only show that each $g_j \in G_j$ fixes $(gi - 1)y_i$. Now by (4), $y_i = f_V(H_i)(x_i)$ and so by (3),

$$(gi - 1)y_i = \prod_{h_i \in H_i} ((gi - 1)(x_i) + (hi - 1)(x_i))$$

which is in $S\langle x_1, \ldots, x_{i-1}\rangle_{F_p}$ and so is fixed by $g_j$ for $j \geq i$. If $j < i$ then $[g_j, g_i] = (g_j^{-1}h^{-1}_i g_j)g_i \in H \cap G_i = H_i$ and so since each element of $H_i$ fixes $y_i$ we see that
$$g_j(g_i - 1)y_i = (g_i g_j - g_j) y_i = (g_i - 1) y_i$$

because $g_j$ fixes $y_i$ by (A). So $(g_i - 1)y_i \in S^G$.

We now let $g \in G$. Then, since $G$ is a $\beta$-Nakajima $p$-group, $g = g_1 \cdots g_n$ with $g_j \in G_j$.

It follows that $g(y_i) = g_1(y_i)$ by repeated use of (A) proved above and since $[g_j, g_i] \in H \cap G_i = H_i$ for $j < i$. The result follows since we have shown above that $(g_i - 1)y_i \in S^G$.

We assume that $(g - 1)y_i \in S^G$, for all $g \in G$. The map $\bar{\epsilon}_i$ from $G$ to the additive group $S^G$ given by $\bar{\epsilon}_i(g) = (g - 1)y_i$ is a homomorphism (using (1)) and so $[G, G] \leq \text{Ker}(\bar{\epsilon}_i)$ for each $i$. By Lemma 2, since $\tilde{H}$ is $\beta$-Nakajima group, $S^\tilde{H} = F_p[y_i \mid 1 \leq i \leq n]$ and so $\tilde{H} = \bigcap_{i=1}^n \text{Ker}(\bar{\epsilon}_i)$. Thus $[G, G] \leq \tilde{H} \leq H$. \hfill $\Box$

We come to the main result of this section.

**Proposition 8.** Suppose $H$ a subgroup of the $\beta$-Nakajima $p$-group $G$ and $[G, G] \leq H$. Let $b \in S^H$ satisfy $(g - 1)b \in S^G$ for all $g \in G$. Then

$$b = \sum_{i \in I} \sum_{j=0}^{m_i-1} b_{ij} y_i^j + b'.$$

Here $b', b_{ij} \in S^G$ for all $i$ and $j$, $I = \{i \mid m_i > 0\}$, and $m_i$ is defined by $[G_i : H_i] = p^{m_i}$.

**Proof.** Since $[G, G] \leq H$ we have $[G, G] \leq \tilde{H}$ by Lemma 3(B). Also, $b \in S^H \subseteq S^\tilde{H}$ and $(\tilde{H}_i) = H_i$ for all $i$. So without loss of generality we may assume that $H = \tilde{H}$ and so is a $\beta$-Nakajima $p$-group.

We use induction on $[G : H]$. If $[G : H] = 1$ there is nothing to prove. So we assume that $[G : H] > 1$. Then for some $m$, $H_m < G_m$. We pick $g_m \in G_m \setminus H_m$. By hypothesis $[G, G] \leq H$ and so $g_m$ normalizes $H$ and since it is of order $p$, $L = \langle g_m, H \rangle$ has order $p \cdot |H|$. Since $H_m < \langle g_m, H_m \rangle \leq L_m$ we have

$$H = H_1 H_2 \cdots H_n < L_1 L_2 \cdots L_n = \bar{L} \leq L.$$

Since $|L| = p \cdot |H|$ it follows that $H_i = L_i$ for all $i \neq m$, $L_m = \langle g_m, H_m \rangle$ and $L = \bar{L}$. So $L$ is a $\beta$-Nakajima $p$-group and also $y_i := N^{L_i}(x_i) = N^{L_j}(x_i)$ for $i \neq m$ and

$$z_m := N^{L_m}(x_m) = N_{H_m}^{L_m}(y_m) = \prod_{\alpha \in F_p} g^n(\alpha y_m) = \prod_{\alpha \in F_p} (\alpha y_m + \alpha(g - 1)y_m)$$

by Lemma 7(B) and use of (1). It follows that

$$z_m = y_m^p - (g_m - 1)y_m^{p-1} y_m.$$ (7)

By Lemma 3, $S^L = F[N^{L_i}(x_i) \mid 1 \leq i \leq n] = F[y_1, z_m \mid i \neq m, 1 \leq i \leq n]$ and $S^H = F[y_1, \ldots, y_n] = S^L[y_m]$. So by Lemma 5(B), $\{y_m^r \mid 0 \leq r \leq p-1\}$ is a basis for $S^H$ over $S^L$. By Lemma 7(B), $(g_m - 1)y_m \in S^G \leq S^L$. Thus by Lemma 4(B) applied to $g_m$
we have \( b = b_0 + b_1 y_m \) with \( b_0, b_1 \in S^L \). Applying \((g_m - 1)\) to this equation we see using Lemma 7(B) that \( b_1 \in S^G \). For \( g \) in \( G \) we now apply \((g - 1)\) to this same equation and conclude, again using Lemma 7(B), that \((g - 1)b_0 \in S^G \). We use the expression for \( z_m \) in (7) and the induction hypothesis applied to \( b_0 \) in \( S^L \) to obtain the result. □

5. Main result

Throughout this section we assume that \( H \) is a subgroup of \( G \) containing \([G, G]\) where \( G \) is a \( \beta \)-Nakajima \( p \)-group and \( \beta = \{x_1, \ldots, x_n\} \) is a basis of \( V \). We note that since \( G = G_1 G_2 \cdots G_n \) and since each \( G_i \) is an elementary abelian \( p \)-group then so also is \( G/[G, G] \).

We denote by \((\overline{\cdot})\) the natural map from \( G \) onto \( \overline{G} := G/H \). Since \( [G, G] \leq H \) we see that \( \overline{G} \) is an elementary abelian \( p \)-group. For \( g \) in \( G \) and \( s \) in \( SH \) we note that \((g - 1)s\) depends only on \( \sigma := \overline{g} \) and so we denote it by \( s_\sigma \). Similarly, for \( g_i \) in \( G_i \), we let \( c_\sigma := (g_i - 1)y_i \) where \( \sigma := \overline{g_i} \) and \( y_i := N^{H_i}(x_i) \).

By Lemma 7(B), \( c_\sigma \) is in \( S^G \). It follows for \( \sigma, \tau \) in \( \overline{G_i} \) that \( c_{\sigma \tau} = c_\sigma + c_\tau \) (8).

**Proof.** By (4), \( y_i = f_{V(H_i)}(x_i) \). We note that each element of \( G_i \) fixes \( V(H_i) := \{(h_i - 1)x_i \mid h_i \in H_i\} \) elementwise. Then

\[
c_{\sigma} = (g_i - 1)y_i \quad \text{where} \quad \sigma := \overline{g_i} \quad \text{and} \quad y_i := N^{H_i}(x_i).
\]

By Lemma 7(B), \( c_{\sigma} \) is in \( S^G \). It follows for \( \sigma, \tau \) in \( \overline{G_i} \) that

\[
c_{\sigma \tau} = c_\sigma + c_\tau.
\]

We let \( \sigma \in \overline{G} \). If \( \sigma \in \overline{G_i} \) for at least one \( i \) we define \( d_\sigma := \operatorname{lcm}_{\sigma \in \overline{G_i}} (c_\sigma) \). Otherwise \( d_\sigma \) is not defined. By Lemma 7(B), \( c_{\sigma} \in S^G \) for each \( i \) and so \( d_\sigma \in S^G \). We note that \( d_\sigma \) is defined only up to a scalar.

**Proposition 9** [2, Theorem 4.4]. Suppose \( H \) is a maximal subgroup of the \( \beta \)-Nakajima \( p \)-group \( G \). Then \( S^H = S^G[a] \) for some homogeneous \( a \) in \( S^H \). If \( \overline{G} = \langle \sigma \rangle \) then \( d_\sigma = d_\sigma = \operatorname{lcm}_{\sigma \in \overline{G}} (c_\sigma) = \operatorname{lcm}_{\sigma \in \overline{G} \setminus H} \langle (g_i - 1)x_i \rangle \) and so is the product of distinct (up to a scalar) elements of \( V \).

**Lemma 10.** Suppose \([G, G] \leq H \leq K < G\), where \( G \) is a \( \beta \)-Nakajima \( p \)-group, and \([G : K] = p\). Let \( \sigma \in \overline{G} \setminus \overline{K} \). Assume \( b \in S^H \) satisfies \( \operatorname{Stab}_{\overline{G}}(b) = H \) and \( b_\sigma \in S^G \) for all \( \sigma \in \overline{G} \). Then \( N_\sigma = \prod_{\tau \in \overline{K}} b_{\sigma \tau} \), where \( N := N^{H}(b) \).
Proof. We let $\varepsilon : \tilde{K} \to S^G$ be defined by $\varepsilon(\tau) = b_{\tau}$. Since $\tilde{K}$ is elementary abelian it is an $F_p$-space. Using (1) we see that $\varepsilon$ is an $F_p$-homomorphism. Since $\text{Stab}_{\tilde{K}}(b) = H$ we see that $\ker(\varepsilon) = 1$.

We set $W := \text{Im}(\varepsilon)$. Then $N = \prod_{\tau \in \tilde{K}}(b + b_{\tau}) = f_W(b)$ since $\ker(\varepsilon) = 1$. So by (3), $N_{\sigma} = f_W(b_{\sigma}) = \prod_{\tau \in \tilde{K}}(b_{\sigma} + b_{\sigma\tau})$. Using (1) we see that $b_{\sigma} + b_{\tau} = b_{\sigma\tau}$ and so $N_{\sigma} = \prod_{\tau \in \tilde{K}} b_{\sigma\tau}$. □

Theorem 11. Suppose $[G, G] \leq H \leq G$ where $G$ is a $B$-Nakajima $p$-group for $B = \{x_1, \ldots, x_n\}$ a basis for $V$. Then the following are equivalent:

(A) $S^H = S^G[b]$ for some homogeneous $b \in S^H$;

(B) there is a homogeneous $b \in S^H$ such that

(i) $b_{\sigma} \in S^G$ for all $\sigma \in \tilde{G}$,

(ii) $S^K = S^G[\sigma N_K(b)]$ for all $K$ such that $H \leq K < G$ and $[G : K] = p$;

(C) for each $\sigma \in \tilde{G}$, $d_{\sigma}$ is defined (equivalent to $\tilde{G} = \bigcup_{\sigma \in \tilde{G}} \tilde{G}$) and there is a homogeneous $b \in S^H$ such that

(i) $(b_{\sigma}, b_{\tau}) = 1$ for all $\sigma, \tau \in \tilde{G}$ provided $\langle \sigma \rangle \neq \langle \tau \rangle$,

(ii) $b_{\sigma} = d_{\sigma}$;

(D) for each $\sigma \in \tilde{G}$, $d_{\sigma}$ is defined and has a fixed value such that for $\sigma, \tau \in \tilde{G}$

(i) $d_{\sigma\tau} = d_{\sigma} + d_{\tau}$ and

(ii) $(d_{\sigma}, d_{\tau}) = 1$ provided $\langle \sigma \rangle \neq \langle \tau \rangle$.

Note that for $\sigma \neq 1$, $d_{\sigma}$ has $p - 1$ values since it is defined only up to a scalar.

Remark. (D)(ii) is equivalent to: For $\{\sigma_1, \ldots, \sigma_m\}$ an arbitrarily chosen basis of $\tilde{G}$, there is a value of each $d_{\sigma_k}$ such that $d_{\sigma} = \sum_{k=1}^{m} \alpha_k d_{\sigma_k}$ where $\alpha_k \in F_p$ for all $k$.

Proof. We show (A) $\iff$ (B) $\iff$ (C) $\iff$ (D) and (B) $\implies$ (A).

(A) $\implies$ (B) is an immediate consequence of Proposition 6.

For $G$ a group we denote $G\setminus\{1\}$ by $G^*$.

Lemma 12. (B)(ii) $\implies$ If $H \leq L < G$ then $\text{Stab}_G(N^L_H(b)) = L$.

Proof of Lemma 12. We assume that $g \in \text{Stab}_G(N^L_H(b)) \setminus L$. Since $G/H$ is an elementary abelian $p$-group there is a maximal subgroup $K$ of $G$ containing $L$ such that $g \notin K$.

For $k, l \in G$, since $G/H$ is abelian, $gkl = kgl$ for some $h \in H$. So if $K$ and $L$ are left transversals of $L$ in $K$ and $H$ in $L$ respectively then

$$g N^K_H(b) = g \prod_{k \in K} k \prod_{l \in L} l(b) = \prod_{k \in K} kg \prod_{l \in L} l(b) = N^K_H(b),$$

since $g$ fixes $N^L_H(b) = \prod_{l \in L} l(b)$. We have thus shown that $g$ fixes $N^K_H(b)$. But $G = \langle g, K \rangle$ and so $N^K_H(b) \in S^G$. But then $S^G = S^G[\sigma N_K(b)]$ which equals $S^K$ by (B)(ii), a contradiction. So $\text{Stab}_G(N^L_H(b)) = L$. □
(B) $\Rightarrow$ (C). We suppose that $\sigma \in \bar{G}^*$. Then there is a maximal subgroup $K$ of $G$ containing $H$ such that $\bar{G} = (\sigma, K)$. By (B)(ii), $S^K = S^G[N]$ where $N := N^\bar{G}_H(b)$. But $S^K = S^G[a]$ by Proposition 9. Since $N$ and $a$ are both homogeneous we see by a degree argument that $N = a + t$ where $t \in S^G$. So $N_\sigma = a_\sigma$.

By Lemma 12, $\text{Stab}_{\bar{G}}(b) = H$ and so we can use Lemma 10 to get

$$\prod_{\omega \in K} b_{\sigma \omega} = N_\sigma = a_\sigma = \text{lcm}_{g_i \in G_i \setminus K_i} \{ (g_i - 1)x_i \}. \quad (9)$$

The last equation is by Proposition 9. We now prove (C)(i) We let $\tau \in \bar{G}^*$ with $\langle \sigma \rangle \neq \langle \tau \rangle$. Since $\bar{G}$ is elementary abelian we could have chosen $K$ such that $\tau \in \bar{K}$. Then by (9), $(b_{\sigma}, b_{\sigma \tau}) = 1$. It follows that $(b_\sigma, b_\tau) = 1$ which is (C)(i).

To prove (C)(ii), we need Lemma 13.

**Lemma 13.** Assume (B)(i) and let $\tau = \bar{g}_i \in \bar{G}_1^*$. Then $(g_i - 1)x_i$ divides $d_\tau$ which in turn divides $b_\tau$.

**Proof.** By (5),

$$c_{\tau i} := (g_i - 1)y_i = \prod_{h_i \in H_i} (g_i h_i - 1)x_i.$$ 

So $(g_i - 1)x_i$ divides $c_{\tau i}$ and so also $d_\tau := \text{lcm}_{i \in H_i} (c_{\tau i})$.

Since by hypothesis $b$ satisfies (B)(i) we can apply Proposition 8 to obtained the expression (6) for $b$. It follows that

$$b_\tau = (g_i - 1)b = \sum_{j=0}^{m_i - 1} h_{ij} c_{\tau i}^{p_j}$$

since $g_i$ fixes $y_k$ for all $k \neq i$ by Lemma 7(A). Thus $c_{\tau i}$ and so also $d_\tau$ divides $b_\tau$. $\square$

We now prove (C)(ii), namely that $b_\sigma = d_\sigma$ for all $\sigma \in \bar{G}$. We first assume that $\sigma \neq 1$. Since $\bar{G}$ is an elementary abelian $p$-group there is a maximal subgroup $K$ of $G$ such that $\sigma \notin K$. Then by (9), $b_\sigma$ is the product of distinct (up to a scalar) linear factors. We let $v$ be an arbitrary such factor. Then for some $i, \nu = (g_i - 1)x_i$ for some $g_i \in G_i \setminus K_i$. We let $\tau := \bar{g}_i \in \bar{G}_1^*$. By Lemma 13, $v$ divides $b_\tau$. But $v$ divides $b_\sigma$ and so by (C)(i) proved above $\langle \sigma \rangle = \langle \tau \rangle$. So $\sigma = \tau^\alpha = \bar{g}_i^\alpha$ for some $\alpha \in F_p^\times$. In particular, $\sigma \in \bar{G}_1^*$ and so $d_\sigma$ is defined. Then by Lemma 13, $(\bar{g}_i^\alpha - 1)x_i = \alpha (g_i - 1)x_i$ on use of (1) divides $d_\sigma$. But $v = (g_i - 1)x_i$ was an arbitrary factor of $b_\sigma$. So $b_\sigma$ divides $d_\sigma$. On the other hand, since we have $\sigma \in \bar{G}_1^*$, by Lemma 13, $d_\sigma$ divides $b_\tau$. Thus $d_\sigma = b_\sigma$ (up to a scalar) for all $\sigma \in \bar{G}_1^*$. Also, $d_1 = 0 = b_1$.

So we have proved (C)(ii) and that $d_\sigma$ is defined for all $\sigma \in \bar{G}$, as required.

(C) $\Rightarrow$ (B). We let $\sigma \in \bar{G}$. Since $c_{\sigma i} \in S^G$, $d_\sigma = b_\sigma \in S^G$. So (B)(i) is true.
We prove (B)(ii). So we assume that $K$ is a maximal subgroup of $G$ containing $H$ and show that $S^K = S^G[N]$ where $N := N^K_H(b)$.

We first show that $\text{Stab}_G(b) = H$. So we let $g \in \text{Stab}_G(b)$ and put $\sigma := \tilde{g}$. Then $0 = (g - 1)b = b_\sigma = d_\sigma$. But $d_\sigma = 0$ only if $\sigma = 1$. So $g \in H$.

We can now use Lemma 10. Since $K$ is maximal in $G$, $\tilde{G} = \langle \sigma, \tilde{K} \rangle$ for some $\sigma \in \tilde{G}$. By Lemma 10 and since $d_\sigma \neq 0$ for all $\tau \in \tilde{K}$,

$$N_{\sigma} = \prod_{\tau \in \tilde{K}} b_{\sigma\tau} = \prod_{\tau \in \tilde{K}} d_{\sigma\tau} \neq 0. \quad (10)$$

We let $\tau \in \tilde{K}$. We denote $\{i \mid \sigma \tau \in \tilde{G} \}$ by $T$. By hypothesis $d_{\sigma\tau} := \text{lcm}_{i \in T}(c_{\sigma\tau i})$ is defined and so $T$ is non-empty. For $i \in T$ we have $c_{\sigma\tau i} = \prod_{h \in H}(g_i h_i - 1)x_i$ by (5) where $g_i = \sigma \tau$ and so $g_i h_i \notin K_i$. It follows that $d_{\sigma\tau}$ is the product of distinct linear factors of the form $(g_i - 1)x_i$ with $g_i \in G_i \setminus K_i$ and $i$ running through $T$. By (C)(i), $(d_{\sigma\tau}, d_{\sigma\tau'}) = 1$ for $\tau \neq \tau'$.

We conclude from (10) that $N_{\sigma}$ is the product of distinct linear factors of the form $(g_i - 1)x_i$ where $g_i \in G_i \setminus K_i$ and $i \in T$.

By Proposition 9, $S^K = S^G[a]$ and $a_{\sigma} = \text{lcm}_{i \in G_i \setminus K_i}(c_{\sigma i})$. So $N_{\sigma}$ divides $a_{\sigma}$. Since $N_{\sigma} \neq 0$ by (10), $\deg N = \deg N_{\sigma} \leq \deg a_{\sigma} = \deg a$. Now $N \in S^K = S^G[a]$ and so by a degree argument, $\deg N = \deg a$ since otherwise $\deg N < \deg a$ and so $N$ would be in $S^G$ which contradicts $N_{\sigma} \neq 0$. It follows that $S^K = S^G[a] = S^G[N]$.

(C) $\Rightarrow$ (D). This is clear since for $\sigma, \tau \in \tilde{G}$, $b_{\tau} = b_{\sigma\tau} \in S^G$ and so by use of (1), $d_{\sigma\tau} = b_{\sigma\tau} + b_{\tau} = d_{\sigma} + d_{\tau}$.

(D) $\Rightarrow$ (C). Our first task is to construct the required $b \in S^H$. It will be of the form given by (6) in Proposition 8. We let $[G_i : H_i] = p_{i}$ and $I = \{i \mid 1 \leq i \leq n, m_i > 0\}$. Throughout the proof we always assume $i \in I$, $1 \leq k \leq m_i$, and $0 \leq j < m_i$. We define $b_{ij}$ as follows. We fix $i \in I$ and pick a basis $[\alpha_{lk} \mid 1 \leq k \leq m_i]$ for $G_i$. We let $A_i$ (respectively $D_i$) be the $m_i \times m_i$ (respectively $m_i \times 1$) matrix with $c_{\alpha_{lk}}$ (respectively $d_{\alpha_{lk}}$) in the $k$-j-th place. We note that by Lemma 7(B), all the entries of $A_i$ and $D_i$ are in $S^G$. We suppose $a_{lk} \in F_p$ ($1 \leq k \leq m_i$) and let $\sigma = \prod_{k=1}^{m_i} \alpha_{lk} \in \tilde{G}_i^\ast$. Then using both (8) and hypothesis (D)(i) we see that

$$\sum_{k=1}^{m_i} a_{lk} \text{ (k-th row of } A_i \text{ (respectively } D_i)) = \text{the row } (c_{\alpha_{lk}}^{p^{m_i}}) \text{(respectively the element } d_{\alpha_{lk}}). \quad (11)$$

Since $\sigma \in \tilde{G}_i^\ast$, in particular $\sigma \neq 1$, there is a $g_i \in G_i \setminus H_i$ such that $\sigma = \tilde{g}_i$. Then $0 \neq \prod_{h \in H_i}(g_i h_i - 1)x_i = (g_i - 1)y_i$ by (5). Thus $c_{\sigma i} := (g_i - 1)y_i \neq 0$ and so by (11) no non-trivial linear combination of the rows of $A_i$ is $0$. So $\det A_i \neq 0$. We let

$$S = \{\sigma \in \tilde{G}_i^\ast \mid \text{one from each non-trivial cyclic subgroup of } \tilde{G}_i\}.$$ 

Since $\tilde{G}_i$ is an elementary abelian $p$-group of order $p^{m_i}$, $S$ has $(p^{m_i} - 1)/(p - 1)$ elements.
By (11), $c_{\sigma i}$ divides $A_i$ for each $\sigma \in \tilde{G}_i^\ast$. However, it follows from (5) that

$$\left(c_{\sigma i}, c_{\tau i}\right) = 1 \quad \text{if} \quad \langle \sigma \rangle \neq \langle \tau \rangle \quad (12)$$

and so $\prod_{\sigma \in S} c_{\sigma i}$ divides $A_i$. Both this product and $A_i$ are homogeneous and of the same degree, namely, $(\deg y_i) (p^m - 1)/(p - 1)$, and so, up to a scalar,

$$\det A_i = \prod_{\sigma \in S} c_{\sigma i}. \quad (13)$$

We denote $A_i^{-1} D_i$ by $(b_{ij}) \ (0 \leq j < m_i)$. So,

$$A_i(b_{ij}) = D_i. \quad (14)$$

Using Cramer’s rule we have $b_{ij} = \det A_{ij}/\det A_i$ where $A_{ij}$ is $A_i$ with its $j$th column replaced by $D_i$. Thus $b_{ij} \in Q(S^G)$. By (11), $c_{\sigma i}$ divides $A_{ij}$ for all $j$ since $c_{\sigma i}$ divides $d_{\sigma i}$.

Then by (12), $\prod_{\sigma \in S} c_{\sigma i}$ divides $A_{ij}$ in $S^G$. Thus by (13), $\det A_i$ divides $\det A_{ij}$ in $S^G$ and so $b_{ij} \in S^G$ for all $i$ and $j$.

We now put

$$b = \sum_{i \in I} \sum_{j=0}^{m_i-1} b_{ij} y_i^j. \quad (15)$$

To complete the proof we must show that $b \in S^H$ and $b_{\sigma} = d_{\sigma}$ for all $\sigma \in \tilde{G}$. We let $g_i \in G_i$ and put $\sigma_i := \tilde{g}_i$. We show that $(g_i - 1)b = d_{\sigma_i}$.

If $i \in I$, then by (15), $A_i(b_{ij}) = D_i$ and so, using (11) we see that

$$\sum_{j=0}^{m_i-1} b_{ij} c_{\sigma_{ni}}^{p'_j} = d_{\sigma_i}. \quad (16)$$

For $l \neq i$, by Lemma 7(A), $g_i$ fixes $y_l$. So applying $(g_i - 1)$ to $b$ as given by (15) we see that $(g_i - 1)b$ is the same sum and so $(g_i - 1)b = d_{\sigma_i}$ for all $i \in I$.

If $i \notin I$, then $g_i \in H_i$. So $\sigma_i = \tilde{g}_i = 1$ and thus $d_{\sigma_i} = 0$. Applying $(g_i - 1)$ to $b$ in (15) we see that $(g_i - 1)b = 0 = d_{\sigma_i}$ as above.

We have thus shown that $(g_i - 1)b = d_{\sigma_i}$ for all $i \ (1 \leq i \leq n)$ and all $g_i \in G_i$ with $\sigma_i = \tilde{g}_i$.

We let $g \in G$. Then $g = g_1 g_2 \cdots g_n$ with $g_i \in G_i$. We put $\sigma = \tilde{g}$ and $\sigma_i := \tilde{g}_i$ for each $i$. Then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_n$. It follows using (1) and since each $d_{\sigma_i} \in S^G$ that $(g - 1)b = \sum_{i=0}^{n} d_{\sigma_i}$ which is equal to $d_{\sigma}$ by hypothesis (D)(i). In particular, if $g \in H$ then $\sigma := \tilde{g} = 1$ and so $(g - 1)b = d_1 = 0$. Thus $b \in S^H$, as required.

It follows that $b_{\sigma}$ is defined and $b_{\sigma} = (g - 1)b = d_{\sigma}$ as proved above. So (D) implies (C).

(B) $\Rightarrow$ (A). We assume (B). We prove (A) by induction on $m$, where $[G : H] = p^m$. For $m = 1$ the result is just a restatement of (B)(ii). So we can suppose that $m \geq 2$. 

---

So we can pick \( \{e_1, e_2\} \subseteq G \) independent mod \( H \). We denote \( \langle e_i, H \rangle \) by \( K_i \) \((i = 1, 2)\). Since \( G/H \) is an elementary abelian \( p \)-group, \([K_i : H] = p\). Clearly \( K_1 \) satisfies the hypotheses of the theorem and using (B)(i) for \( b \) we see that \( N \) satisfies (B)(ii). Also by (B)(ii) for \( H \) we see that \( K_1 \) satisfies (B)(iii). So by the induction hypothesis \( S_{K_1} = S^G[N] \).

We assume \( S^H \neq S^G[b] \) and obtain a contradiction. Lemma 12, Stab\(_C(b) = H \) and thus by Lemma 5(A), \( Q(S^G_1[b]) = Q(S^H) \). So there is a non-zero \( f \in S^G \) and \( d \in S^H \setminus S^G[b] \) such that \( fd \in S^G[b] \). We may clearly assume that \( f \) is irreducible in the polynomial ring \( S^G \). We fix one such \( f \).

Since \( \text{Stab}_G(b) = H \), by Lemma 5(B), \( \{b^i \mid 1 \leq i < p\} \) is a basis of \( S^K_1[b] \) over \( S^{K_1} \).

We let \( d \in S^H \setminus S^G[b] \) be such that \( fd \in S^G[b] \) and is of minimal degree \( r \) in \( b \) over \( S^{K_1} \). So \( fd = \sum_{i=0}^{r-1} d_i b^i \) uniquely, where \( d_i \in S^{K_1} \) all \( i \) and \( d_r \neq 0 \). We denote \( \tilde{e}_1 \) by \( \sigma_1 \). Since \( e_1 \) normalizes \( H \), \( \langle e_1 - 1 \rangle d \in S^H \) and

\[
  f(e_1 - 1)d = \sum_{i=0}^{r} d_i \left\{ (b + b_{\sigma_1})^i - b^i \right\} = rd_r b_{\sigma_1}^{r-1} + s,
\]

where \( s \) is a unique sum of terms of lower degree in \( b \) over \( S^{K_1} \). By the minimality of \( r \) we have \( (e_1 - 1)d \in S^G[b] \). It follows that \( f \) divides \( d_r b_{\sigma_1} \).

We first show by contradiction that \( f \) does not divide \( d_r \). So we suppose that \( f \) divides \( d_r \), say \( d_r = fd_r' \). So \( d_r' \in S^{K_1} = S^G[N] \subseteq S^G[b] \). It follows that \( f(d - d_r' b^r) \in S^G[b] \) and so by the minimality of \( r \) we have \( d - d_r' b^r \in S^G[b] \) and so \( d \) is also, a contradiction. Thus \( f \) does not divide \( d_r \).

We note that although \( f \) divides \( d_r b_{\sigma_1} \) and does not divide \( d_r \) this does not immediately imply that \( f \) divides \( b_{\sigma_1} \), since although \( f \) is irreducible in \( S^G \) it might not be irreducible in \( S^{K_1} \).

We show that \( f \) divides \( b_{\sigma_2} \). By Lemma 12 with \( L = K_1 \), we have \( \text{Stab}_G(N) = K_1 \) and so using Lemma 5(B) \( \{N^i \mid 0 \leq i < [G : K_1]\} \) is a basis for \( S^{K_1} = S^G[N] \) over \( S^G \). So \( d_r = \sum_{i=0}^{d_k} c_i N^i \) uniquely, where \( c_i \in S^G \) for all \( i \). Since \( f \) divides \( d_r b_{\sigma_1} \) and \( b_{\sigma_1} \in S^G \) by hypothesis (B)(ii), it follows that \( f \) divides \( c_i b_{\sigma_1} \) for all \( i \). Since \( f \) does not divide \( d_r \) it does not divide \( c_k \) for some \( k \). It follows that \( f \) divides \( b_{\sigma_1} \), similarly, \( f \) divides \( b_{\sigma_2} \).

Since we chose \( \{e_1, e_2\} \) to be independent mod \( H \) and \( \sigma_i = e_i \) \((i = 1, 2)\) we have \( \langle \sigma_1 \rangle \neq \langle \sigma_2 \rangle \).

We have proved that (B) \( \Rightarrow \) (C). By (C)(i), \( (b_{\sigma_1}, b_{\sigma_2}) = 1 \). This contradicts the fact that \( f \) divides both \( b_{\sigma_1} \) and \( b_{\sigma_2} \). So our assumption that \( S^H \neq S^G[b] \) is false. Thus \( S^H = S^G[b] \) which is (A).

We have completed the proof of Theorem 11. \( \square \)

6. When is \( S^H = S^G[b] \) a polynomial algebra?

For a homogeneous element \( z \) of a graded algebra we denote by \( |z| \) its degree.

We suppose that \( V \) is an \( n \)-dimensional vector space over a field \( F \) and we let \( S = S(V) \) be the symmetric algebra of \( V \).

The main result of this section is Proposition 16. We need
**Proposition 14.** Let $G$ be a finite subgroup of $GL(V)$ such that $S^G = F[z_1, \ldots, z_n]$ is a polynomial algebra, where each $z_i$ is homogeneous. Let $H$ be a proper subgroup of $G$ with $S^H = S^G[b]$ where $b$ is homogeneous.

(A) Suppose there exists a group $L$ with $H \leq L < G$ such that $S^L$ is a polynomial algebra. Then so also is $S^H$.

(B) (i) Suppose $S^H$ is a polynomial algebra. Then there is an integer $k$ ($1 \leq k \leq n$) such that

$$S^H = F[b, z_i \mid i \neq k].$$

(ii) Suppose in addition that $ch F = p$, $G$ is a $p$-group and $H \triangleleft G$. Then for $H \leq L \leq G$, $S^L = F[N^H_L(b), z_i \mid i \neq k]$. 

**Proof.** (A) Let $S^L = F[u_1, \ldots, u_n]$ where each $u_i$ is homogeneous. We assume that $S^H$ is not a polynomial algebra and get a contradiction. It follows from this assumption that \{z_1, \ldots, z_n, b\} and {u_1, \ldots, u_n, b} are minimal homogeneous generating sets for $S^H = S^G[b] = S^L[b]$. So after an, if necessary, reordering of the $u_i$, $|z_i| = |u_i|$ for all $i$. But $|G| = \prod_i |z_i| = \prod_i |u_i| = |L|$ and so $L = G$, a contradiction. Thus $S^H$ is a polynomial algebra.

(B)(i) We let $S^H = F[u_1, \ldots, u_n]$ where each $u_i$ is homogeneous. We put $T := S^H/(S^H)^2$. Then $T$ is a vector space over $F$ of dimension $n$. We let $(\sim) := S^H_T \rightarrow T$ be the natural map. We denote $\{\bar{u_1}, \ldots, \bar{u_n}\}$ by $U$ and $\{\bar{z_1}, \ldots, \bar{z_n}, \bar{b}\}$ by $W$. Then $U$ is a basis of, and $W$ spans $T$. For $d$ a positive integer we denote by $T_d$ the $F$-subspace of $T$ of all the elements of degree $d$. Then $U_d := U \cap T_d$ is a basis of, and $W_d = W \cap T_d$ spans, $T_d$. It follows that there is exactly one integer $d$ for which there is a linear relation among the elements of $W_d$. But $b$ cannot appear in this relation since otherwise $b$ would be in $F[z_1, \ldots, z_n] = S^G$ which is impossible since $H$ is a proper subgroup of $G$.

(B)(ii) By (B)(i) just proved, $S^H = F[b, z_i \mid i \neq k]$. For $g \in G$, since $H \triangleleft G$, $g(b) \in S^H$. Since $b$ is homogeneous and $g$ has order a power of $p$, a simple argument shows that $(g-1)b \in F[z_i \mid i \neq k]$.

Now $N^L_H(b) := \prod_{z \in L} g(b) = \prod_{z \in L} (b + (g-1)b)$ where $L$ is a left transversal of $H$ in $L$. It follows that $b$ is integral over $F[A]$ where $A = \{N^L_H(b), z_i \mid i \neq k\}$. Thus $S^H$ is integral over $F[A]$ and so $A$ is a homogeneous system of parameters (hsop) in $S^L$. Since $S^H = F[b, z_i \mid i \neq k]$ is a polynomial algebra, $H = |b| \prod_{i \neq k} |z_i|$ by [9, Corollary 5.5.4, p. 124]. On the other hand, the product of the degrees of the elements of the hsop $A$ is $([L : H]|b|) \prod_{i \neq k} |z_i| = [L : H]|H| = |L|$. It follows from [9, Proposition 5.5.5, p. 125] that $S^L = F[N^L_H(b), z_i \mid i \neq k]$. □

**Lemma 15.** Suppose $F = F_p$. Let $H$ be a proper normal subgroup of the B-Nakajima $p$-group $G$ where $B = \{x_1, \ldots, x_n\}$ such that $S^H = S^G[b]$ for $b \in S^H$ homogeneous. Suppose there exists $k$ ($1 \leq k \leq n$) such that $m = m_k$ where $p^m = [G : H]$, $p^{m_k} := [G_k : H_k]$ and $|b| = |y_k|$ where $y_k := N^{H_k}(x_k)$.

Then for $\sigma \in G^k_k$, $b_\sigma = c_{\sigma k}$ where $c_{\sigma k} := (g_k - 1)y_k$ with $g_k = \sigma$, $g_k \in G_k$. 

**I.P. Hughes, N. Kechagias / Journal of Algebra 291 (2005) 72–89**
Proof. By Proposition 6(A)(i), \((g - 1)b \in S^G\) for all \(g \in G\). So by Proposition 8,

\[
b = \sum_{i \in I} \sum_{j=0}^{m_i-1} b_{ij} y_i^j + b',
\]

where \(b_{ij}, b' \in S\) for all \(i, j\) and the notation is as in that proposition, since \(m_k = m > 0\), \(k \in I\). By hypothesis \(|b| = |y_k|\) and so \(b_{kj} = 0\) for \(j > 0\) and \(\alpha := b_{k0} \in F_p\). We show that \(\alpha \neq 0\). Since \(m_k > 0\) there is a \(g_k \in G_k \setminus H_k\). Applying \((g_k - 1)\) to \(b\) in (16) we see, since \(g_k\) fixes \(y_i\) for all \(i \neq k\), that \((g_k - 1)b = \alpha(g_k - 1)y_k\). If \(\alpha = 0\) then \(g_k \in \text{Stab}_G(b) = H\) by Lemma 5(A), a contradiction. So \(\alpha \neq 0\).

We let \(\sigma \in G_k^x\). Then \(\sigma = g_k\) for some \(g_k \in G_k \setminus H_k\) and so by the argument above, \(b_\sigma = (g_k - 1)b = (g_k - 1)y_k = c_{\sigma k}\).

Proposition 16. Assume \(F = F_p\) and let \(H\) be a proper normal subgroup of the \(\beta\)-Nakajima \(p\)-group \(G\) where \(\beta = \{x_1, \ldots, x_n\}\) a basis for \(V\) over \(F = F_p\). Suppose \(S^H = S^G[b]\) where \(b\) is homogeneous. Then the following are equivalent:

(A) \(S^H\) is a polynomial algebra;
(B) for some \(k\) \((1 \leq k \leq n)\),

(i) \(m = m_k\) where \([G : H] = p^m\) and \([G_k : H_k] = p^{m_k}\),

(ii) For all \(\sigma \in G_k^*\), \(d_\sigma = \text{lcm}\}_{[\alpha \in G_k^*](c_{\sigma k})} = c_{\alpha k}\), where \(\alpha\) is the natural map from \(G\) onto \(G/H\). \(c_{\sigma k} = (g_k - 1)y_k\) with \(\bar{g}_k = \sigma\), and \(y_i := N^{H_k}(x_i)\).

Proof. Since \(S^H = S^G[b]\), by Proposition 6(A)(ii), \([G, G] \leq H\). We prove that (A) and (B) are equivalent by induction on \(m\) where \(p^m := [G : H]\). For \(m = 1\) this equivalence is just a restatement of [2, Corollary 4.5]. So we assume that \(m > 1\).

(A) \(\Rightarrow\) (B)(i). We let \(k\) be the integer of Proposition 14(B)(i). We pick \(g \in G \setminus H\) such that when \(m_k = [G_k, H_k] > 0\), \(g = g_k \in G_k\). We let \(L = (g, H)\). Since \(G/[G, G]\) is elementary abelian and \([G, G] \leq H, L \lhd G\) and \([L : H] = p\). By Proposition 6(B), \(S[L] = S^G[N_H^G(b)]\) and from Proposition 14(B)(ii), \(S[L]\) is a polynomial algebra. So we can apply the inductive hypothesis to \(L\) to get \(p^{m-1} = [G : L]\). If \(m_k > 0\), since \(g = g_k \in G_k\), \([G_k : H_k] = L_k\) and so \([G_k : L_k] = p^{m_k-1}\). It follows that \(m = m_k\), as required. If \(m_k = 0\), \([G_k : L_k] = 1\) and so \(m = 1\), which contradicts our assumption that \(m > 1\). So we have proved (B)(i).

(A) \(\Rightarrow\) (B)(ii). By Lemma 2, \(S^G = F_p\{z_i | 1 \leq i \leq n\}\) where \(z_i := N^{G_k}(x_i)\). But also \(S^G = F_p[N_H^G(b), z_i | i \neq k]\) by Proposition 14(B)(ii). It follows that \([N_H^G(b)] = |z_k|\) and so since \(m = m_k\), \(|b| = |y_k|\) where \(y_k := N^{H_k}(x_k)\). We now apply Lemma 15 to get (B)(ii).

(B) \(\Rightarrow\) (A). Since \(m > 1\) there is an \(L < G\) such that \(H < L\). Since \([G, G] \leq H, L < G\). By Proposition 6(B), \(S[L] = S^G[N_H^G(b)]\). So \(L\) satisfies the hypotheses of the proposition. We show that \(L\) satisfies (B).

(B)(i) Since \(m = m_k\), \([G : H] = [G_k : H_k]\) and so \([G : L] = [G_k : L_k]\).

(B)(ii) Since \(1 < p^{m_k} = |G_k|\) we can pick \(\sigma \in G_k^*\). Then \(b_\sigma = d_\sigma\) by Theorem 11(C)(ii). Thus
\[ |b| = |\beta| = |a| |d| \quad \text{by (B)(ii)} \]

\[ c_k \quad \text{by (B)(ii)} \]

So,
\[ |N^L_H(b)| = [L : H] \cdot |b| = [L_k : H_k] \cdot |y_k| \]

We have shown that \( L \) satisfies the hypotheses of Lemma 15, and so it satisfies (B)(ii). Thus by the inductive hypothesis, \( S^L \) is a polynomial algebra. Applying Lemma 14(A) we see that \( S^H \) is a polynomial algebra. \( \square \)

7. Examples

We construct an infinite set of pairs of groups \((G, H)\) which satisfy the hypotheses of Theorem 10 and so \( S^H = S^G[b] \).

For \( V \) a vector space we denote \( V \setminus \{0\} \) by \( V^* \).

We suppose \( U \) and \( W \) are vector spaces over \( F \) of dimension \( m \geq 1 \) and \( r \geq 1 \), respectively. We also let \( T \) be the vector space over \( F \) with basis \( J = \{ x, x(u+w) \mid u \in U^*, w \in W^* \} \).

So \( \dim T = (p^m - 1)(p^r - 1)/(p - 1) + 1 \).

We now put \( V := U \oplus W \oplus T \). We let \( \{ x_1, \ldots, x_m \} \) and \( \{ x_{m+1}, \ldots, x_{m+r} \} \) be bases of \( U \) and \( W \), respectively. In \( J \) we label \( x \) as \( x_{m+r+1} \) and the other elements of \( J \) arbitrarily as \( \{ x_{m+r+2}, \ldots, x_n \} \). We denote the basis \( \{ x_1, \ldots, x_T \} \) of \( V \) by \( \beta \).

We now define the corresponding pair \((G, H)\). For \( u \in U \), we define \( g_u \) by

\[ (g_u - 1)(x) = u \quad \text{and} \quad g_u \text{ fixes } x_i, \forall x_i \neq x \]

and for \( u \in U^* \) and \( w \in W^* \) we define \( g_{u+w} \) by

\[ (g_{u+w} - 1)(x((u+w))) = u + w \quad \text{and} \quad g_{u+w} \text{ fixes } x_i, \forall x_i \neq x((u+w)) \]

We note that \( g_0 = 1 \).

We now let

\[ G := \langle g_u, g_{u+w} \mid u, v \in U^*, w \in W^* \rangle \]

and

\[ H := \langle g_u g_{u+w} \mid u \in U^*, w \in W^* \rangle. \]

It is clear that \( V^G = V^H = U \oplus W \) and that \( G \) is a \( \beta \)-Nakajima \( p \)-group which is elementary abelian. For \( \alpha \in F_p^* \) we have \( g_{\alpha u} = g_u^\alpha \) and \( g_{\alpha u + \alpha w} = g_{u+w}^\alpha \) and so most of the generators for \( G \) and \( H \) given above are redundant. Clearly, \( \text{rank}(G) = m + \ldots \)
\[(p^m - 1)(p^r - 1)/(p - 1)\text{ and } [G : H] = p^m.\] We let \((\cdot)\) be the natural map from \(G\) onto \(G/H\).

We now show that \((G, H)\) satisfies (D) of Theorem 11.

We prove (D)(i). From the definitions of \(G\) and \(H\) above we see that

(a) \(H_i = 1\) for all \(i\) and so if \(\sigma = \tilde{g}_i \in \tilde{G}_i^*\) then \(c_{\sigma i} := (g_i - 1)N^H(x_i) = (g_i - 1)x_i\).

(b) Let \(\sigma \in \tilde{G}^*\). Then, since \(\tilde{G} = \tilde{G}_{m+r+1}\), \(\sigma = \tilde{g}_u\) for some \(u \in U\). Also, for \(i \neq m + r + 1\), \(\sigma \in \tilde{G}_i^*\) if and only if \(x_i \in \{\lambda(u + w) \mid w \in W\}\). It follows from (a) and (b) that if \(\sigma \in \tilde{G}^*\) then

\[
d_{\sigma} := \text{lcm}_{\sigma \in \tilde{G}_i} = \prod_{w \in W}(u + w)
\]

which is equal to \(f_W(u)\) from the definition of \(f_W(X)\) in (2). Also, \(d_1 = 0\). We let \(\sigma, \tau \in \tilde{G}\). Then \(\sigma = \tilde{g}_u\) and \(\tau = \tilde{g}_v\) for unique \(u, v \in U\). So \(d_{\sigma} + d_{\tau} = f_W(u) + f_W(v) = f_W(u + v) = d_{\sigma \tau}\) since \(g_u g_v = g_{u+v}\).

To prove (D)(ii) we let \(\tau \in \tilde{G}^*\). Then, as above, \(\sigma = \tilde{g}_v\) for some \(v \in U^*\). If \(\langle \sigma \rangle \neq \langle \tau \rangle\) then \(\langle u \rangle_{F_p} \neq \langle v \rangle_{F_p}\) and so \(d_{\sigma} = (f_W(u), f_W(v)) = 1\) as required.

Thus \((G, H)\) satisfies (D) of Theorem 11 and so \(S^H = S^G[b]\) where \(b\) is a homogeneous element of \(S^H\) and, if needed, can be explicitly written down. By Theorem 11(C)(ii), \(b_{\sigma} = d_{\sigma} \) and so \(|b| = |b_{\sigma}| = |d_{\sigma}| = p^r\) for \(\sigma \neq 1\) by (17). Since \(|c_{\sigma i}| \leq 1\) for all \(\sigma \in \tilde{G}\), by (a) above \(d_{\sigma} \neq c_{\sigma i}\) for any \(i\) so (B)(ii) of Proposition 16 is false. Thus \(S^H\) is not a polynomial algebra.

It is clear that \(G\) and \(H\) depend only on \(m\) and \(r\) and so we denote them by \(G(m, r)\) and \(H(m, r)\), respectively.

By Lemma 2, \(S^{G(m, r)} = F_p[N^G(x_i) \mid 1 \leq i \leq n]\). So, since \(S^{H(m, r)} = S^{G(m, r)}[b]\) is not a polynomial algebra, \(\{N^G(x_i) ; b \mid 1 \leq i \leq n\}\) is a minimal generating set. It follows that the degrees of the elements of any minimal generating set of \(S^{H(m, r)}\) are

\[
|N^G(x_i)| = \begin{cases} 
1, & \text{for } 1 \leq i \leq m + r, \\
p^m, & i = m + r + 1, \\
p, & m + r + 1 \leq i \leq n.
\end{cases}
\]

It is clear that \(S^{H(m, r)}\) is not isomorphic to \(S^{H(m', r')}\) if \((m, r) \neq (m', r')\). Similarly we see that if \(\text{min}(r, m) > 1\) then \(S^{H(m, r)}\) cannot be equal to \(S^M[a]\) for any group \(M \subseteq GL(V)\) (with polynomial invariant ring) containing \(H(m, r)\) such that \([M : H(m, r)] = p\). So \(S^{H(m, r)}\) is not covered by Theorem 4.4 of [2].

In summary, we have shown that for each pair of positive integers \((m, r)\) where \(\text{min}(r, m) > 1\) we have constructed a Nakajima \(p\)-group \((G(m, r))\) which is elementary abelian and a subgroup \(H(m, r)\) such that \(S^{H(m, r)} = S^{G(m, r)}[b]\) for some \(b \in S^{H(m, r)}\) and is not a polynomial ring. If \((m, r) \neq (m', r')\) then the corresponding invariant rings are not isomorphic.
Acknowledgments

We thank Eddy Campbell, Jianjun Chuai and David Wehlau for their help. We also thank the referee for pointing out mathematical errors in an earlier version of this paper.

References