110. *Modular Representations of p-Groups with Regular Rings of Invariants*

By Haruhisa NAKAJIMA
Department of Mathematics, Keio University

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1980)

§1. **Introduction.** Let V be an n-dimensional vector space over a field k of characteristic p and G a finite subgroup of $GL(V)$. Then G acts linearly on the symmetric algebra R of V. We denote by R^G the subring of R consisting of all invariant polynomials under this action of G. The following theorem is well known.

(1.1) **Theorem** (Chevalley-Serre, cf. [2], [3], [5]). *Suppose that* $p=0$ *or* $(|G|, p)=1$. *Then* R^G *is a polynomial ring if and only if* G *is generated by pseudo-reflections in* $GL(V)$ *(an element* σ *of* $GL(V)$ *is said to be a pseudo-reflection if* rank $(\sigma-1)\leqq 1$).

Now we assume that $p>0$ and that the order of G is divisible by p. Serre obtained a necessary condition for R^G to be a polynomial ring as follows.

(1.2) **Theorem** (Serre, cf. [2], [5]). *If* R^G *is a polynomial ring, then* G *is generated by pseudo-reflections.*

However the converse of (1.2) is not always true. For example $R^{O_n(F_q)}$ $(n\geqq 4$, p odd) are not polynomial rings, where $O_n(F_q)$ are orthogonal subgroups of $GL(V)$ of dimension n defined over the subfield F_q of k consisting of q elements.

Hereafter we suppose that k is the prime field of characteristic $p(>0)$ and that G is a p-subgroup of $GL(V)$.

The purpose of this note is to announce our results on rings of invariants of p-groups. We can completely determine p-groups G such that R^G are polynomial rings. The main result is

(1.3) **Theorem.** *The following statements on a pair of* V *and* G *are equivalent:*

(1) R^G *is a polynomial ring.*

(2) *There is a* k*-basis* $\{X_1, \cdots, X_n\}$ *of* V *with the equality*

$$\prod_{i=1}^{n} |GX_i| = |G|$$

such that all $\oplus_{i=1}^{j} kX_i$ $(1\leqq j\leqq n)$ *are* kG*-submodules of* V.

In [1] it has been shown that if G is a p-Sylow subgroup of $GL(V)$, R^G is a polynomial ring.

§2. **Preliminaries.** We need some lemmas on invariant subrings of polynomial rings:

(2.1) **Lemma.** *Let N be a subgroup of $GL(V)$ and let H be the inertia group of a prime ideal $\mathfrak{p}$ of R under the natural action of N. If R^N is a polynomial ring, then R^H is also a polynomial ring.*

Proof. It suffices to treat the case where $\mathfrak{p}$ is generated by

$$\mathfrak{p} \cap V.$$

Then we easily see that

$$\left[\bar{k} \underset{k}{\otimes} R^H\right]_{\mathfrak{m}_1} \cong \left[\bar{k} \underset{k}{\otimes} R^H\right]_{\mathfrak{m}_2}$$

for any maximal ideals $\mathfrak{m}_i$ of $\bar{k} \otimes_k R^H$ which contain $\mathfrak{p}^H$, where $\bar{k}$ denotes the algebraic closure of k. On the other hand, since $\mathfrak{p}^H$ is unramified over $\mathfrak{p} \cap R^N$, $R^H_{\mathfrak{p}^H}$ is a regular local ring. This implies that $\bar{k} \otimes_k R^H$ is a polynomial ring. Hence R^H is also a polynomial ring.

For a subset A of a ring S, $\langle A \rangle_S$ denotes the ideal of S generated by A.

(2.2) **Lemma.** *For a subgroup N of $GL(V)$ let W be a kN-submodule of V with $[V/W]^N = V/W$. Then $R^N/[\langle W \rangle_R]^N$ is a polynomial ring.*

Proof. The additive group $\bar{k} \otimes_k V/W$ acts transitively on the set consisting of closed points in the support of the $\bar{k} \otimes_k R^N$-module $\bar{k} \otimes_k R^N/[\langle W \rangle_R]^N$. Therefore $R^N/[\langle W \rangle_R]^N$ is a polynomial ring.

(2.3) **Lemma.** *Suppose that N and W are the same as in* (2.2). *Furthermore let W contain a kN-submodule $\tilde{W}$ such that* $\dim W/\tilde{W} = 1$. *Then $[R^H/[\langle \tilde{W} \rangle_R]^H]^{N/H}$ is a polynomial ring where H denotes the inertia group of $\langle \tilde{W} \rangle_R$ under the action of N.*

This follows easily from (2.2).

(V, H), which is called a *couple*, stands for a pair of a group H and an H-faithful kH-module V such that V/V^H is a nonzero trivial kH-module (i.e., H acts trivially on the nonzero vector space V/V^H, and so H is an elementary abelian p-group). (U, L) is said to be a *subcouple* of (V, H) if L is a subgroup of H and U is a kL-submodule of V. Further we say that (V, H) *decomposes* to subcouples (V_i, H_i) $(1 \leqq i \leqq m)$ if $H = \oplus_{i=1}^m H_i$, $V^H \subseteqq V_i \subseteqq V^{H_j}$ for all $1 \leqq i, j \leqq m$ with $i \neq j$ and V/V^H $(= \sum_{i=1}^m V_i/V^H) = \oplus_{i=1}^m V_i/V^H$.

(2.4) **Lemma.** *Suppose that a couple (V, H) decomposes to subcouples (V_i, H_i) $(1 \leqq i \leqq m)$. Then R^H is a polynomial ring if and only if $R_i^{H_i}$ $(1 \leqq i \leqq m)$ are polynomial rings, where each R_i is the symmetric algebra of V_i.*

Proof. The "if" part of (2.4) is obvious. So we assume that R^H is a polynomial ring. Then the ideal $[\langle V^H \rangle_R]^H$ of R^H is generated by V^H. From this we obtain

$$[\langle V_i^{H_i} \rangle_{R_i}]^{H_i} = \langle V_i^{H_i} \rangle_{R_i^{H_i}} \qquad (1 \leqq i \leqq m),$$

since the canonical kH_i-epimorphism $V \to V_i$ induces a graded epimorphism $R^H \to R_i^{H_i}$. Hence, by (2.2), $R_i^{H_i}$ $(1 \leqq i \leqq m)$ are polynomial rings.

A couple (V, H) is defined to be *indecomposable* if it does not decompose to subcouples (V_i, H_i) $(1 \leqq i \leqq m)$ with $m \geqq 2$.

The following theorem, which is a special case of (1.3), plays an essential role in § 3.

(2.5) **Theorem** (cf. [4]). *Let (V, H) be an indecomposable couple. Then R^H is a polynomial ring if and only if* $\dim V/V^H = 1$.

By (1.2), (2.4) and (2.5) we can classify abelian subgroups H of $GL(V)$ such that R^H are polynomial rings (cf. [4]).

(2.6) **Lemma.** *Suppose that for a subgroup N of $GL(V)$ W is a kN-submodule of V. If R^N is a polynomial ring, then $R^N/[\langle W\rangle_R]^N$ is also a polynomial ring.*

Using (2.2), we can easily prove this.

Now let $\{X_1, \cdots, X_n\}$ be a k-basis of V such that all $\oplus_{i=1}^{j} kX_i$ $(1 \leqq j \leqq n)$ are kG-submodules of V. The condition (2) of (1.3) is characterized by

(2.7) **Proposition.** *The following conditions are equivalent*:

(1) $\prod_{i=1}^{n} |GX_i| = |G|$.

(2) *There exist subgroups G_i $(1 \leqq i \leqq n)$ of G such that $GX_i = G_iX_i$ and $G_iX_j = \{X_j\}$ for all $1 \leqq i, j \leqq n$ with $i \neq j$. (In this case $G = G_1 \cdots G_n$.)*

(3) *There exist homogeneous polynomials $f_i \in k[X_1, \cdots, X_i]$ $(1 \leqq i \leqq n)$ such that $R^G = k[f_1, \cdots, f_n]$ and each f_i is divisible by X_i in R.*

The implications (2)$\Rightarrow$(1)$\Rightarrow$(3) are easy. The result (1.2) of Serre is used in the proof of (3)$\Rightarrow$(2).

By (2.3) and the Galois descent, we obtain

(2.8) **Proposition.** *The following conditions are equivalent*:

(1) *R^G is a polynomial ring.*

(2) *There exists an n-dimensional graded polynomial subalgebra $S = k[f_1, \cdots, f_n]$ of R^G with*

$$\prod_{i=1}^{n} \deg f_i \leqq |G|$$

such that $S \cap \sum_{i=1}^{j} RX_i = \sum_{i=1}^{j} Sf_i$ for all $1 \leqq j \leqq n$, where f_i are homogeneous polynomials.

§ 3. **The main theorem.** We adopt the following notation and terminology: Put $V_0 = V$ and for any integer $j \geqq 1$ define $V^j = V_{j-1}^G$, $V_j = V_{j-1}/V^j$ respectively. As G is unipotent, $V_j = V^j = 0$ for sufficiently large j. Let $\underline{X} = \{X_i \mid i \in I\}$ be a k-basis of V. The set $\underline{X}$ is said to be a k-basis relative to G if, for each j $(\geqq 1)$ with $V^j \neq 0$, there is a subset of $\underline{X}$ whose canonical image in V_{j-1} is a k-basis of V^j.

In this section we will give an outline of the proof of a stronger result than (1.3).

(3.1) **Theorem.** *The following statements on a pair of V and G are equivalent*:

(1) *R^G is a polynomial ring.*

(2) *There is a k-basis $\{X_i \mid i \in I\}$ of V relative to G which satisfies the equality*

$$\prod_{i\in I} |GX_i| = |G|.$$

It suffices to show the implication (1)⇒(2) of this theorem. So we suppose that R^G is a polynomial ring and will prove the assertion (2) by induction on the order of G.

If $G=\{1\}$, there is nothing to prove. Thus we assume $G \neq \{1\}$. Let M be a subspace of V^{m-1} such that $\dim V^{m-1}/M = 1$ where $m = \max\{j \mid V^j \neq 0\}$. Further let H be the inertia group of the prime ideal of R generated by $\varphi_{m-2}^{-1}(M)$ under the natural action of G. Here φ_{m-2} is the canonical epimorphism $V \to V_{m-2}$. Then we may assume that $|G| > |H|$. By (2.1) R^H is a polynomial ring. Hence, using the induction hypothesis, we have a k-basis $\{Y_i \mid i \in I\}$ of V relative to H which satisfies

$$\prod_{i\in I} |HY_i| = |H|.$$

On the other hand, from (2.4), (2.5), (2.6) and (2.7), we get

(3.2) **Proposition.** *If for a k-basis $\{Z_i \mid i \in I\}$ of V relative to G the equality*

$$\prod_{i\in I} |HZ_i| = |H|$$

holds, then there exists another k-basis $\{Z'_i \mid i \in I\}$ of V relative to G such that

$$\prod_{i\in I} |GZ'_i| = |G|.$$

To prove our theorem we need only to construct a k-basis $\{Z_i \mid i \in I\}$ of V relative to G with

$$\prod_{i\in I} |HZ_i| = |H|.$$

Let us put

$$J = \{i \in I \mid |HY_i| < |HY_{j(i)}| \text{ for some } j(i) \in I\}$$

and set $U = \oplus_{i\in J} kY_i$. Then U is a kG-submodule of V. By (2.8) we infer that A^G is a polynomial ring where A denotes the symmetric algebra of U. Let $\rho: G \to GL(U)$ be the representation of G associated with the kG-module U. As $|G/\mathrm{Ker}\,\rho| < |G|$, from the induction hypothesis we find a k-basis $\{Z_i \mid i \in J\}$ of U relative to $G/\mathrm{Ker}\,\rho$ with

$$\prod_{i\in J} |GZ_i| = |G/\mathrm{Ker}\,\rho|.$$

Clearly there are bases of V relative to G which contain $\{Z_i \mid i \in J\}$ respectively. Moreover, using (2.4) and (2.5), we can prove

(3.3) **Lemma.** *There are elements Z_i $(i \in I \backslash J)$ with*

$$\prod_{i\in I\backslash J} |HZ_i| = |H \cap \mathrm{Ker}\,\rho|$$

such that $\{Z_i \mid i \in I\}$ is a k-basis of V relative to G.

The set $\{Z_i \mid i \in I\}$ is a k-basis of V as desired. Thus the proof of

(3.1) is completed.

Detailed accounts will be published elsewhere.

References

[1] M.-J. Bertin: Sous-anneaux d'invariants d'anneaux de polynomes. C. R. Acad. Sci. Paris, **260**, 5655–5658 (1965).

[2] N. Bourbaki: Groupes et algèbres de Lie. Chs. 4, 5 et 6, Herman, Paris (1968).

[3] C. Chevalley: Invariants of finite groups generated by reflections. Amer. J. Math., **67**, 778–782 (1955).

[4] H. Nakajima: Modular representations of abelian groups with regular rings of invariants (to appear in Nagoya Math. J.).

[5] J.-P. Serre: Groupes finis d'automorphismes d'anneaux locaux réguliers. Colloq. d'Alg. E. N. S. (1967).