H. Nakajima
Nagoya Math. J.
Vol. 86 (1982), 229-248

MODULAR REPRESENTATIONS OF ABELIAN GROUPS WITH REGULAR RINGS OF INVARIANTS

HARUHISA NAKAJIMA

§ 1. Introduction

Let k be a field of characteristic p and G a finite subgroup of $GL(V)$ where V is a finite dimensional vector space over k. Then G acts naturally on the symmetric algebra $k[V]$ of V. We denote by $k[V]^G$ the subring of $k[V]$ consisting of all invariant polynomials under this action of G. The following theorem is well known.

THEOREM 1.1 (Chevalley-Serre, cf. [1, 2, 3]). *Assume that $p = 0$ or $(|G|, p) = 1$. Then $k[V]^G$ is a polynomial ring if and only if G is generated by pseudo-reflections in $GL(V)$.*

Now we suppose that $|G|$ is divisible by the characteristic $p(> 0)$. Serre gave a necessary condition for $k[V]^G$ to be a polynomial ring as follows.

THEOREM 1.2 (Serre, cf. [1, 3]). *If $k[V]^G$ is a polynomial ring, then G is generated by pseudo-reflections in $GL(V)$.*

But the ring $k[V]^G$ of invariants is not always a polynomial ring, when G is generated by pseudo-reflections in $GL(V)$ (cf. [1, 3]).

In this paper we shall completely determine abelian groups G such that $\boldsymbol{F}_p[V]^G$ are polynomial rings ($\boldsymbol{F}_p$ is the field of p elements). Our main result is

THEOREM 1.3. *Let V be a vector space over $\boldsymbol{F}_p$ and G an abelian group generated by pseudo-reflections in $GL(V)$. Let G_p denote the p-part of G and assume that $G_p \neq \{1\}$. Then the following statements on G are equivalent:*

(1) *$\boldsymbol{F}_p[V]^G$ is a polynomial ring.*

(2) *The natural $\boldsymbol{F}_p G_p$-module V defines a couple (V, G_p) which decomposes to one dimensional subcouples (for definitions, see § 2).*

Received June 19, 1980.

The computation of invariants of elementary abelian p-groups G plays an essential role in the proof of this theorem. Therefore we need to study the structure of $\boldsymbol{F}_pG$-modules V such that $\boldsymbol{F}_p[V]^G$ are polynomial rings under some additional hypothesis (see § 3). In § 4 our main result shall be reduced to (3.2).

Hereafter k stands for the prime field of characteristic $p > 0$ and without specifying we assume that all vector spaces are defined over k.

§ 2. Preliminaries

An element σ of $GL(V)$ is said to be a *pseudo-reflection* if $\dim(1-\sigma)V \leqq 1$. We say that a graded ring $R = \oplus_{n\geqq 0}R_n$ is *defined over* a field K, when $R_0 = K$ and R is a finitely generated K-algebra. It is well known that R is a polynomial ring over K if R is regular at the homogeneous maximal ideal $\oplus_{n>0}R_n$. For a subset A of a ring R, $\langle A\rangle_R$ denotes the ideal of R generated by A. To simplify our notation we put $\langle A\rangle = \langle A\rangle_{k[V]}$ if A is a subset of the fixed k-space V (for a subset B of a group, $\langle B\rangle$ means the subgroup generated by B).

PROPOSITION 2.1. *Let G be an abelian group generated by pseudo-reflections in $GL(V)$ and let G_p denote the p-part of G. Then $k[V]^G$ is a polynomial ring if and only if $k[V]^{G_p}$ is a polynomial ring.*

Proof. Let $\bar{k}$ be the algebraic closure of k and let $G_{p'}$ be the p'-part of G. Since G is an abelian group generated by pseudo-reflections in $GL(\bar{k}\otimes_k V)$, we can immediately find a $\bar{k}G_p$-submodule V_p and a $\bar{k}G_{p'}$-submodule $V_{p'}$ such that $V_p \subseteqq (\bar{k}\otimes_k V)^{G_{p'}}$, $V_{p'} \subseteqq (\bar{k}\otimes_k V)^{G_p}$ and $\bar{k}\otimes_k V = V_p \oplus V_{p'}$. Therefore

$$\bar{k}\otimes_k k[V]^G \cong \bar{k}[\bar{k}\otimes_k V]^G \cong \bar{k}[V_p]^{G_p} \otimes_{\bar{k}} \bar{k}[V_{p'}]^{G_{p'}}$$

and $\bar{k}[V_{p'}]^{G_{p'}}$ is a polynomial ring. The assertion follows from these facts, because $k[V]^G$ and $\bar{k}[V_p]^{G_p}$ are graded algebras defined over fields.

PROPOSITION 2.2. *If G is an abelian p-group generated by pseudo-reflections in $GL(V)$, then V/V^G is a trivial kG-module (i.e. G acts trivially on V/V^G).*

Proof. Let $\sigma \in G - \{1\}$ be a pseudo-reflection and choose $Z \in V$ to satisfy $(1-\sigma)V = kZ$. Clearly it suffices to prove that $Z \in V^G$. Since G

is abelian, $\tau(kZ) = (1-\sigma)\tau(V) = kZ$ for any element τ of G. Hence the map $\chi\colon G \to k^*$ defined by

$$\tau \longmapsto \frac{\tau^{-1}(Z)}{Z}$$

is a group homomorphism, where k^* is the unit group of k. But we have $\operatorname{Hom}(G, k^*) = \{1\}$, as G is a p-group. This implies that $Z \in V^G$.

(V, G), which is called a *couple*, stands for a pair of a group G and a G-faithful kG-module V such that V/V^G is a nonzero trivial kG-module (in this case G is an elementary abelian p-group). The *dimension* of (V, G) is defined to be $\dim V/V^G$. We say (U, H) is a *subcouple* of (V, G) if H is a subgroup of G and U is a kH-submodule of V. Let us associate (V, G) with the subspace

$$\mathscr{A}(V, G) = \sum_{\sigma \in G} (1-\sigma)V$$

of V^G and the subring $\mathscr{Q}(V, G)$ which is the image of the canonical ring homomorphism

$$k[V]^G/\langle V^G\rangle^G \longrightarrow k[V/V^G]\ .$$

LEMMA 2.3. *For any couple (V, G) the k-algebra $\mathscr{Q}(V, G)$ is a polynomial ring.*

Proof. Putting

$$R = \bar{k}[\bar{k} \otimes_k V]^G/(\langle \bar{k} \otimes_k V^G\rangle_{\bar{k}[\bar{k}\otimes_k V]})^G\ ,$$

we see that

$$R \cong \bar{k} \otimes_k \mathscr{Q}(V, G)$$

as graded algebras defined over $\bar{k}$. Let $\mathfrak{M}_i$ $(i = 1, 2)$ be maximal ideals of $\bar{k}[\bar{k} \otimes_k V]$ which contain the ideal $\langle \bar{k} \otimes_k V^G\rangle_{\bar{k}[\bar{k}\otimes_k V]}$. Then, by the definition of a couple, we can select a coordinate transform

$$\rho\colon \bar{k}[\bar{k} \otimes_k V] \longrightarrow \bar{k}[\bar{k} \otimes_k V]$$

sending $\mathfrak{M}_1$ to $\mathfrak{M}_2$ which commutes with the action of G. The contractions of $\mathfrak{M}_i$ $(i = 1, 2)$ to $\bar{k}[\bar{k} \otimes_k V]^G$ define maximal ideals $\mathfrak{N}_i$ of R respectively and the transform φ induces $R_{\mathfrak{N}_1} \cong R_{\mathfrak{N}_2}$. Hence we conclude that R is regular, because it is an affine domain. From this $\mathscr{Q}(V, G)$ is a polynomial ring.

We say that (V, G) decomposes to subcouples (V_i, G_i) $(1 \leqq i \leqq m)$ if $G = \oplus_{1\leqq i\leqq m} G_i$, $V^G \subsetneqq V_i \subsetneqq V^{G_j}$ for all $1 \leqq i, j \leqq m$ with $i \neq j$ and

$$V/V^G\Big(= \sum_{1\leqq i\leqq m} V_i/V^G\Big) = \bigoplus_{1\leqq i\leqq m} V_i/V^G .$$

The set consisting of these subcouples is called a *decomposition* of (V, G). Further (V, G) is defined to be *decomposable*, when it has a decomposition $\{(V_i, G_i): 1 \leqq i \leqq m\}$ with $m \geqq 2$.

PROPOSITION 2.4. *Let (V, G) be a couple which decomposes to subcouples (V_i, G_i) $(1 \leqq i \leqq m)$. Then the following conditions are equivalent*:

(1) *$k[V]^G$ is a polynomial ring.*

(2) *$k[V_i]^{G_i}$ $(1 \leqq i \leqq m)$ are polynomial rings.*

Proof. Suppose that $k[V]^G$ is a polynomial ring. Since $k[V]^G$ contains $k[V_i]^{G_i}$, the canonical kG_i-epimorphism $V \to V_i$ induces a graded epimorphism

$$\psi_i\colon k[V]^G \longrightarrow k[V_i]^{G_i} .$$

Clearly $V^G = V_i^{G_i}$ and $\psi_i(\langle V^G\rangle^G) = (\langle V^G\rangle_{k[V_i]})^{G_i}$. Hence $\langle V^G\rangle^G = \langle V^G\rangle_{k[V]^G}$ implies

$$(\langle V_i^{G_i}\rangle_{k[V_i]})^{G_i} = \langle V_i^{G_i}\rangle_{k[V_i]^{G_i}} .$$

By (2.3) we see that $\mathcal{Q}(V_i, G_i)$ are polynomial rings and therefore $k[V_i]^{G_i}$ $(1 \leqq i \leqq m)$ are also polynomial rings. Conversely we assume the condition (2). Denote by n_i the dimension of (V_i, G_i) $(1 \leqq i \leqq m)$ and let f_{ij} $(1 \leqq j \leqq n_i)$ be homogeneous polynomials in $k[V_i]$ such that $k[V_i]^{G_i} = k[V_i^{G_i}][f_{i1}, \cdots, f_{in_i}]$ $(1 \leqq i \leqq m)$. Then it follows easily that $k[V]^G = k[V^G][f_{ij}\colon 1 \leqq i \leqq m, 1 \leqq j \leqq n_i]$.

For a one dimensional couple $(V^G \oplus kX, G)$ we call

$$F(X) = \prod_{\sigma\in G} \sigma(X)$$

the *canonical $(V^G \oplus kX, G)$-invariant on X.* $F(X)$ satisfies the identity

$$F(Y_1 + Y_2) = F(Y_1) + F(Y_2) .$$

Clearly we must have $k[V^G \oplus kX]^G = k[V^G][F(X)]$ and hence

COROLLARY 2.5. *If a couple (V, G) decomposes to one dimensional subcouples, then $k[V]^G$ is a polynomial ring.*

PROPOSITION 2.6. *Let G be a subgroup of $GL(V)$ and let H be the* *inertia group of a prime ideal* $\mathfrak{P}$ *of* $k[V]$ *under the natural action of* G. *If* $k[V]^G$ *is a polynomial ring, then* $k[V]^H$ *is also a polynomial ring.*

This proposition is almost evident.

LEMMA 2.7. *Let* (V, G) *be a couple with* $\dim V^G = 1$ *and suppose that* $\{X_i : 0 \leqq i \leqq m\}$ *is a k-basis of* V *with* $V^G = kX_0$. *Further, for non-negative integers* $t(i)$ $(1 \leqq i \leqq m)$, *let* R *be the graded polynomial subalgebra* $k[X_0, X_1^{pt(1)}, \cdots, X_m^{pt(m)}]$ *of* $k[V]$. *Then* R^G *is a polynomial ring and we can effectively determine a regular system of homogeneous parameters of* R^G.

Proof. We prove this by induction on $|G|$ and may assume that

$$\begin{aligned} t(1) = \cdots < \cdots &= t(m_{i-1}) < t(m_{i-1} + 1) \\ &= t(m_{i-1} + 2) \cdots = t(m_i) < \cdots < \cdots = t(m_n) \end{aligned}$$

where m_n is equal to m. Let us put

$$U_i = \bigoplus_{0 \leqq j \leqq m_1} kX_j^{pt(m_i)}$$

and

$$U_i' = U_i \oplus \bigoplus_{m_{i-1} < j \leqq m_i} kX_j^{pt(m_i)}$$

respectively and moreover define G_1 to be the stabilizer of G at U_1. Then there is a subgroup G_2 such that $G = G_1 \oplus G_2$. Because U_i is a G_2-faithful kG_2-module with $(G_2 - 1)U_i = kX_0^{pt(m_i)}$, we deduce that the natural short exact sequence

$$0 \longrightarrow U_i \longrightarrow U_i' \longrightarrow \bigoplus_{m_{i-1} < j \leqq m_i} kX_j^{pt(m_i)} \bmod U_i \longrightarrow 0$$

of kG-modules is G_2-split. Therefore we may suppose that $X_j^{pt(m_i)}$ $(2 \leqq i \leqq n;$ $m_{i-1} < j \leqq m_i)$ are invariants of G_2. On the other hand we can effectively determine homogeneous polynomials f_i $(1 \leqq i \leqq m_1)$ which satisfy $k[U_1]^{G_2} = k[X_0^{pt(m_1)}, f_1, \cdots, f_{m_1}]$. Hence it follows that $R^G = S^{G_1}[f_1, \cdots, f_{m_1}]$ where $S = k[X_0][X_j^{pt(m_i)} : 2 \leqq i \leqq n,\ m_{i-1} < j \leqq m_i]$. Then the assertion is shown from the induction hypothesis.

When W is a kH-submodule of U for a subgroup H of $GL(U)$, we denote by $H(W)$ the kernel of the canonical homomorphism $H \to GL(U/W)$.

PROPOSITION 2.8. *Let* (V, G) *be a couple such that* $k[V]^G$ *is a polynomial ring. Then we can effectively determine a regular system of homogeneous parameters of* $\mathcal{Q}(V, G)$.

Proof. Let

$$0 = W_0 \subseteqq W_1 \subseteqq \cdots \subseteqq W_d = V^G$$

be an ascending chain of subspaces with $\dim W_i/W_{i-1} = 1$. Put $R_0 = k[V]$ and define

$$R_i = R_{i-1}^{G_i}/W_i R_{i-1}^{G_i} \qquad (1 \leqq i \leqq d)$$

inductively where G_i denotes $G(W_i)$. Then obviously the natural map

$$\mathscr{Q}(V, G) \longrightarrow R_d$$

is an isomorphism, because, by (2.6), $k[V]^{G_i}$ $(1 \leqq i \leqq d)$ are polynomial rings. Hence this proposition follows from (2.7).

LEMMA 2.9. *Let (V, G) be a one dimensional couple and suppose that $\{X, T_1, \cdots, T_d\}$ is a k-basis of V with $V^G = \oplus_{1 \leqq i \leqq d} kT_i$. Further let $F(X)$ denote the canonical (V, G)-invariant on X. If $\oplus_{i \neq 1} kT_i \not\supseteqq \mathscr{A}(V, G)$ and $\oplus_{i \neq 2} kT_i \supseteqq \mathscr{A}(V, G)$, then we have $F(T_1) \in \langle T_2, T_3, \cdots, T_d \rangle$ and*

$$F(X) \equiv X^{p^u} - T_1^{p^u - p^{u-1}} X^{p^{u-1}} \bmod \langle T_3, T_4, \cdots, T_d \rangle$$

where $p^u = |G|$.

Proof. Choose a k-basis $\{Z_j : 1 \leqq j \leqq u\}$ of $\mathscr{A}(V, G)$ such that $Z_1 \equiv T_1 \bmod \oplus_{i \neq 1} kT_i$ and $\oplus_{i \neq 1} kT_i \supseteqq \{Z_2, Z_3, \cdots, Z_u\}$. Putting $F_1(X) = X^p - Z_u^{p-1} X$, we inductively define

$$F_{i+1}(X) = F_i(X)^p - F_i(Z_{u-i})^{p-1} F_i(X) \qquad (i < u)\ .$$

Then there exist elements σ_i $(1 \leqq i \leqq u)$ in G which satisfy $(\sigma_i - 1)X = Z_i$ and therefore we must have $F(X) = F_u(X)$. From this we deduce that

$$\begin{aligned} F(T_1) &= F_{u-1}(T_1)^p - F_{u-1}(Z_1)^{p-1} F_{u-1}(T_1) \\ &\equiv 0 \bmod \langle T_2, T_3, \cdots, T_d \rangle \end{aligned}$$

and

$$\begin{aligned} F(X) &= F_{u-1}(X)^p - F_{u-1}(Z_1)^{p-1} F_{u-1}(X) \\ &\equiv X^{p^u} - T_1^{p^u - p^{u-1}} X^{p^{u-1}} \bmod \langle T_3, T_4, \cdots, T_d \rangle\ , \end{aligned}$$

since $Z_1 \equiv T_1 \bmod \oplus_{3 \leqq i \leqq d} kT_i$ and $F_{u-1}(X) \equiv X^{p^{u-1}} \bmod \langle T_3, T_4, \cdots, T_d \rangle$.

Let $\mathscr{D} = \{(V^G \oplus W_i, G_i) : 1 \leqq i \leqq m\}$ be a decomposition of (V, G) and put $\operatorname{supp}_{\mathscr{D}} L = \{i_0 : V^G \oplus \oplus_{i \neq i_0} W_i \not\supseteqq L\}$ for a subset L of V. Let us consider an element θ of $GL(V)$ with the property that $V^{\langle \theta \rangle} \supseteqq V^G$. We say θ is

$\mathscr{D}$-admissible if G contains some subgroups G'_i $(1 \leqq i \leqq m)$ which give another decomposition $\mathscr{D}' = \{(V^G \oplus \theta(W_i), G'_i): 1 \leqq i \leqq m\}$ of (V, G). In the case of $\dim W_i = 1$ the transform θ is characterized by

PROPOSITION 2.10. *If $W_i = kX_i$ $(1 \leqq i \leqq m)$ then the following conditions are equivalent:*

(1) *θ is $\mathscr{D}$-admissible.*

(2) *There is a permutation π on $\{1, 2, \cdots, m\}$ such that $|G_i| = |G_{\pi(i)}|$, $\mathscr{A}(V^G \oplus W_{\pi(i)}, G_{\pi(i)}) \supseteqq \mathscr{A}(V^G \oplus W_j, G_j)$ $(j \in \operatorname{supp}_{\mathscr{D}} \theta(W_i))$ and $\pi(i) \in \operatorname{supp}_{\mathscr{D}} \theta(W_i)$ for $1 \leqq i \leqq m$.*

Proof. Suppose that the condition (2) is satisfied and let G'_{i_0} be

$$\{\tau \in GL(V): V^{\langle\tau\rangle} \supseteqq V^G \oplus \bigoplus_{i \neq i_0} \theta(W_i) \text{ and } \mathscr{A}(V^G \oplus W_{\pi(i_0)}, G_{\pi(i_0)}) \supseteqq (1-\tau)V\}$$

for $1 \leqq i_0 \leqq m$. Furthermore set

$$J = \{i: \mathscr{A}(V^G \oplus W_i, G_i) \supseteqq \mathscr{A}(V^G \oplus W_{\pi(i_0)}, G_{\pi(i_0)})\}$$

and

$$J' = \{i: \mathscr{A}(V^G \oplus W_i, G_i) = \mathscr{A}(V^G \oplus W_{\pi(i_0)}, G_{\pi(i_0)})\} .$$

Since $G'_{i_0} \neq \{1\}$, we pick up any element σ from $G'_{i_0} - \{1\}$. Then, for each $j \in J$, we can choose $\tau_j \in G_j$ with $(1 - \tau_j)V = (1 - \sigma)V$. Clearly there are integers $0 \leqq \mu(j) < p$ $(j \in J')$ such that

$$\Big(1 - \prod_{j \in J'} \tau_j^{\mu(j)}\Big)\theta(X_i) = (1 - \sigma)\theta(X_i)$$

for $\pi(i) \in J'$. Further let us define integers $0 \leqq \mu(j) < p$ $(j \in J - J')$ to satisfy

$$\prod_{j \in J} \tau_j^{\mu(j)} \theta(X_i) = \theta(X_i) \qquad (\pi(i) \in J - J') .$$

Consequently we see that

$$\Big(1 - \prod_{j \in J} \tau_j^{\mu(j)}\Big)\theta(X_i) = (1 - \sigma)\theta(X_i) \qquad (1 \leqq i \leqq m) ,$$

which yields

$$\sigma = \prod_{j \in J} \tau_j^{\mu(j)} .$$

Thus the couple (V, G) decomposes to $(V^G \oplus \theta(W_i), G'_i)$ $(1 \leqq i \leqq m)$ since $G \supseteqq G'_i$ and $|G_i| = |G'_i|$ $(1 \leqq i \leqq m)$.

Conversely assume that (V, G) has another decomposition $\mathscr{D}' = \{(V^G \oplus \theta(W_i), G'_i): 1 \leqq i \leqq m\}$ and let $f_i(\theta(X_i))$ be the canonical $(V^G \oplus \theta(W_i), G'_i)$-invariant on $\theta(X_i)$. If

$$\theta(X_i) = \sum_{1 \leqq j \leqq m} a_{ij} X_j$$

for some $a_{ij} \in k$, we have

$$f_i(\theta(X_i)) = \sum_{1 \leqq j \leqq m} a_{ij} f_i(X_j)\ .$$

Select a subgroup H_{ij} of $GL(V^G \oplus W_j)$ such that $k[V^G \oplus W_j]^{H_{ij}} = k[V^G][f_i(X_j)]$. Then the natural kH_{ij}-module $V^G \oplus W_j$ defines a couple which satisfies that $\mathscr{A}(V^G \oplus W_j, H_{ij}) = \mathscr{A}(V^G \oplus \theta(X_i), G'_i)$. On the other hand $f_i(\theta(X_i))$ can be expressed as

$$f_i(\theta(X_i)) = \sum_{1 \leqq j \leqq m} a_{ij} h_{ij} + g_i$$

for $g_i \in \langle V^G \rangle_{k[V]^G}$ and $h_{ij} \in k[V^G \oplus W_j]^{G_j}$ where each h_{ij} is monic as a polynomial of X_j. Therefore the canonical $(V^G \oplus W_j, G_j)$-invariant $F_j(X_j)$ on X_j divides $f_i(X_j)$ in $k[V^G \oplus W_j]$ $(j \in \mathrm{supp}_{\mathscr{D}}\, \theta(X_i))$. From this we must have $\mathscr{A}(V^G \oplus \theta(W_i), G'_i) \supseteqq \mathscr{A}(V^G \oplus W_j, G_j)$ $(j \in \mathrm{supp}_{\mathscr{D}}\, \theta(X_i))$ for $1 \leqq i \leqq m$. The remainder of (2) follows directly from the equality

$$k[V^G][F_1(X_1), \cdots, F_m(X_m)] = k[V^G][f_1(\theta(X_1)), \cdots, f_m(\theta(X_m))]\ .$$

We say that (V, G) is *homogeneous* when $\mathscr{Q}(V, G)$ is homogeneous concerning the natural graduation induced from that of $k[V]$ (i.e. $\mathscr{Q}(V, G)$ is generated by some homogeneous part as a k-algebra). A couple (V, G) is defined to be *quasi-homogeneous* if there is a subspace W of V^G with $\mathrm{codim}_{V^G} W = 1$ such that $G(W) = \{1\}$ or $(V, G(W))$ is a homogeneous subcouple which satisfies $\dim(V, G) = \dim(V, G(W))$.

§ 3. Computation of invariants

Let $(V^G \oplus kX_i, H_i)$ $(1 \leqq i \leqq m)$ be subcouples of (V, G) with

$$\dim(V^G + \sum_{1 \leqq i \leqq m} kX_i) = m + \dim V^G$$

such that $V^{H_j} \ni X_i$ $(i \neq j)$ and $G(W) = \oplus_{1 \leqq i \leqq m} H_i$ for a subspace W of V^G with $\mathrm{codim}_{V^G} W = 1$. We define Z, T_i and W_j to satisfy $V^G = W \oplus kZ$, $W = \oplus_{1 \leqq i \leqq d} kT_i$ and $kX_j = W_j$ $(1 \leqq j \leqq m)$ respectively. $F_i = F_i(X_i)$ denotes the canonical $(V^G \oplus W_i, H_i)$-invariant on X_i. For any n and $c = (c_1, \cdots, c_n) \in \mathbf{Z}^n$, let $\|c\|$ denote the sum $\sum_{1 \leqq i \leqq n} c_i$ and $\{e_i: 1 \leqq i \leqq n\}$ be the standard basis of $\boldsymbol{Z}^n$ ($\boldsymbol{Z}$ is the set of all integers). Further we suppose that there are pseudo-reflections $\sigma_j \in G - G(W)$ $(1 \leqq j \leqq m)$ with $[\lambda_{ij}] \in GL_m(k)$ where

$$\lambda_{ij} = \frac{(\sigma_j - 1)X_i \bmod W}{Z \bmod W}\,.$$

LEMMA 3.1. *Let R be a subalgebra of $k[V]^G$ which contains $k[V^G]$. Assume that $F_1^{c_1}F_2^{c_2}\cdots F_m^{c_m}$ $(0 \leqq c_i < p)$ are linearly independent over R and let g_1 be an element of the R-module*

$$\bigoplus_{c \in \Gamma} RF_1^{c_1}F_2^{c_2}\cdots F_m^{c_m}$$

where $\Gamma = \{c = (c_1, \cdots, c_m) \in \boldsymbol{Z}^m : 0 \leqq c_i < p \text{ and } \|c\| > 1\}$. Then $g_1 = 0$ if $g_1 + g_2 \in k[V]^G$ for a polynomial $g_2 \in k[V]$ with $(\sigma_j - 1)g_2 \in R$ $(1 \leqq j \leqq m)$.

Proof. For $\gamma = (\gamma_1, \cdots, \gamma_m) \in \boldsymbol{Z}^m$ with $0 \leqq \gamma_i < p$ let

$$\Psi_\gamma : \bigoplus_{0 \leqq c_i < p} RF_1^{c_1}F_2^{c_2}\cdots F_m^{c_m} \longrightarrow RF_1^{\gamma_1}F_2^{\gamma_2}\cdots F_m^{\gamma_m}$$

denote the canonical projection. Choose an element $\xi = (\xi_1, \cdots, \xi_m) \in \Gamma$ such that $\Psi_\gamma(g_1) = 0$ at each $\gamma \in \Gamma$ with $\|\gamma\| > \|\xi\|$. We may assume that $\xi_1 > 0$. Besides we define $\eta = (\eta_1, \cdots, \eta_m)$ as $\xi - e_1$ and put $\partial_i\eta = \eta + e_i$ $(1 \leqq i \leqq m)$. Then clearly

$$\Psi_\eta((\sigma_j - 1)g_1) = \Psi_\eta((1 - \sigma_j)g_2) = 0\,,$$

because $(\sigma_j - 1)g_2 \in R$ and $\eta \neq 0$. Further, as

$$(\sigma_j - 1)F_i(X_i) = F_i((\sigma_j - 1)X_i) \in k[V^G]$$

and $k[V]^G \supseteqq R$, we have

$$\begin{aligned}(0 =)\Psi_\eta((\sigma_j - 1)g_1) &= \sum_{\substack{\gamma \in \Gamma \\ \|\gamma\| \leqq \|\eta\| + 1}} \Psi_\eta((\sigma_j - 1)\Psi_\gamma(g_1)) \\ &= \sum_{1 \leqq i \leqq m} \Psi_\eta((\sigma_j - 1)\Psi_{\partial_i\eta}(g_1)) \\ &= \sum_{\eta_i < p-1} (\eta_i + 1)F_i((\sigma_j - 1)X_i)\Psi_{\partial_i\eta}(g_1)F_i(X_i)^{-1}\end{aligned}$$

for all $1 \leqq j \leqq m$. On the other hand the polynomials

$$F_i((\sigma_j - 1)X_i) - \lambda_{ij}F_i(Z) \qquad (1 \leqq i, j \leqq m)$$

are contained in $k[W]$ and hence the terms of $\Psi_\eta((\sigma_j - 1)g_1)$ with variables Z, T_i, X_j whose degrees are maximal on Z are also terms of

$$\sum_{\eta_i < p-1} \lambda_{ij}(\eta_i + 1)F_i(Z)\Psi_{\partial_i\eta}(g_1)F_i(X_i)^{-1}\,,$$

where X_j $(j > m)$ are defined such that $\{Z, T_i, X_j\}$ is a k-basis of V. This implies that

$$\Psi_{\partial_{17}}(g_1)(= \Psi_{\xi}(g_1)) = 0 .$$

Now let us study a decomposition of (V, G) in the case where $m \geqq 2$, $V = V^G \oplus \oplus_{1 \leqq i \leqq m} W_i$, $G(W) = \oplus_{1 \leqq i \leqq m} H_i$ and $|H_i| = p^t$ $(1 \leqq i \leqq m)$ (observe that (V, G) is quasi-homogeneous). The rest of this section is devoted to the proof of the following proposition.

PROPOSITION 3.2. *If $k[V]^G$ is a polynomial ring, then (V, G) is decomposable.*

I_s $(1 \leqq s \leqq \nu)$ stand for equivalence classes of $I = \{1, 2, \cdots, m\}$ with respect to the relation $\sim$ induced by $i \sim j$ when $\mathscr{A}(V^G \oplus W_i, H_i) = \mathscr{A}(V^G \oplus W_j, H_j)$. For each I_s there is a subset J_s of I with $|I_s| = |J_s|$ such that the submatrix $[\lambda_{ij}]_{(i,j) \in I_s \times J_s}$ $(1 \leqq s \leqq \nu)$ is non-singular (J_s $(1 \leqq s \leqq \nu)$ are not always disjoint). We may assume that $[\lambda_{ij}]_{(i,j) \in I_s \times J_s}$ $(1 \leqq s \leqq \nu)$ are monomial matrices, replacing a decomposition of (V, H) consisting of one dimensional subcouples by the use of an admissible transform.

Moreover suppose that $k[V]^G$ is a polynomial ring over k. Since

$$\mathscr{Q}(V, G) \underset{\text{can}}{\cong} (k[V]^{G(W)}/\langle W\rangle^{G(W)})^{G/G(W)}/Z(k[V]^{G(W)}/\langle W\rangle^{G(W)})^{G/G(W)}$$

we have $k[V]^G = k[V^G][f_1, \cdots, f_m]$ for homogeneous polynomials $f_i \in k[V]$ with $f_i \equiv F_i^p \bmod \langle V^G\rangle^{G(W)}$. Then it follows from (3.1) that

$$f_i = F_i^p + \sum_{1 \leqq j \leqq m} F_j h_{ij} \qquad (1 \leqq i \leqq m)$$

where h_{ij} are homogeneous in $k[V^G]$.

We wish to claim $h_{ij} = 0$ $(i \neq j)$ and show this only for the case of $i = 1$. Suppose that T_i $(1 \leqq i \leqq t)$ span the subspace $\mathscr{A}(V^G \oplus W_1, H_1)$ of V^G and set

$$Z_j = Z + \sum_{1 \leqq u \leqq d} b_{ju} T_u \in (\sigma_j - 1)V$$

where $b_{ju} \in k$. For $c = (c_1, \cdots, c_d) \in N^d$ and $g \in k[V^G]_{(p^t+1)}$, $\Phi_c(g) \in k$ is defined to be the coefficient of

$$T_1^{c_1} T_2^{c_2} \cdots T_d^{c_d} Z^{p^t+1-\|c\|}$$

in g which is regarded as a polynomial of T_i $(1 \leqq i \leqq d)$ and Z (N is the set of all non-negative integers). Especially we denote by $a_i(c)$ the value $\Phi_c(Z^{p^t} h_{1i})$.

LEMMA 3.3. *Let c be an element of N^d such that $\|c\| < p^t$. Then we have*

$$a_i(c) = \begin{cases} -1 & \text{if } i = 1 \text{ and } c = 0 \\ 0 & \text{otherwise}. \end{cases}$$

Proof. Suppose that an element $c \in N^d$ satisfies $\|c\| < p^t$. Then

$$\Phi_c(F_1(Z)^p) = \begin{cases} 1 & (c = 0) \\ 0 & (c \neq 0), \end{cases}$$

since $p^{t+1} - \|c\| > p^t$ and

$$F_1(Z) = Z^{p^t} + \sum_{1 \leqq i \leqq t} F_{1i} Z^{p^{t-i}}$$

for $F_{1i} \in k[W]$. On the other hand we have

$$\begin{aligned}(0 =)\Phi_c((\sigma_j - 1)f_1) &= \Phi_c(F_1((\sigma_j - 1)X_1)^p) + \sum_{1 \leqq i \leqq m} \Phi_c(F_i((\sigma_j - 1)X_i)h_{1i}) \\ &= \lambda_{1j}\Phi_c(F_1(Z)^p + \sum_{1 \leqq u \leqq d} b_{ju}F_1(T_u)^p) \\ &\quad + \sum_{1 \leqq i \leqq m} \lambda_{ij}\{\Phi_c(F_i(Z)h_{1i}) + \sum_{1 \leqq u \leqq d} b_{ju}\Phi_c(F_i(T_u)h_{1u})\} \\ &= \lambda_{1j}\Phi_c(F_1(Z)^p) + \sum_{1 \leqq i \leqq m} \lambda_{ij}\Phi_c(F_i(Z)h_{1i}).\end{aligned}$$

Therefore this system is reduced to

$$\sum_{1 \leqq i \leqq m} \lambda_{ij}\Big\{a_i(c) + \sum_{\substack{c' \in N^d \\ 0 < \|c'\| < \|c\|}} \alpha(c')a_i(c')\Big\} = \begin{cases} -\lambda_{1j} & (c = 0) \\ 0 & (c \neq 0) \end{cases}$$

where $\alpha(c') \in k$. The assertion follows from the last equations, because the matrix $[\lambda_{ij}]$ is non-singular.

LEMMA 3.4. *Let L be the subset of*

$$\underbrace{\{0\} \times \cdots \times \{0\}}_{t \text{ times}} \times N^{d-t}$$

consisting of all non-zero elements c such that

$$\|c\| = \omega_0 p^t + \sum_{1 \leqq i \leqq t} \omega_i (p^t - p^{i-1})$$

for $\omega_i \in \boldsymbol{Z}$ with $\omega_i \leqq 0$ $(0 \leqq i \leqq t-1)$ and $0 < \omega_t < p$. If $c \in L$ then $a_j(c) = 0$ $(1 \leqq j \leqq m)$.

Proof. Let $c = (c_1, \cdots, c_d)$ be an element of L such that $a_j(c') = 0$

$(1 \leqq j \leqq m)$ for all $c' \in L$ with $\|c\| > \|c'\|$. Obviously the equalities $\Phi_c(F_1((1-\sigma_j)X_1)^p) = 0$ and $\Phi_c(F_1(Z)h_{11}) = a_1(c)$ follow from $p^{t+1} > \|c\|$ and $(c_1, \cdots, c_t) = 0$. Further we can show that

$$\Phi_c(F_i(Z)h_{1i}) - a_i(c) = \beta_i(0)a_i(0) + \sum_{\substack{c' \in L \\ \|c\| > \|c'\|}} \beta_i(c')a_i(c') \qquad (1 < i \leqq m)$$

for some $\beta_i(0)$, $\beta_i(c') \in k$, because

$$F_i(Z) = Z^{p^t} + \sum_{1 \leqq j \leqq t} F_{ij} Z^{p^{t-j}}$$

where F_{ij} are homogeneous polynomials in $k[W]$. According to (3.3) $a_i(0) = 0$ $(1 < i \leqq m)$ and therefore we must have

$$\Phi_c\Big(\Big(F_i(Z) + \sum_{1 \leqq u \leqq d} b_{ju} F_i(T_u)\Big)h_{1i}\Big) = a_i(c)$$

because $\|c\| \neq p^t$. Now the system

$$\Phi_c(F_1((1-\sigma_j)X_1)^p) = \sum_{1 \leqq i \leqq m} \Phi_c(F_i((\sigma_j - 1)X_i)h_{1i})$$

can be expressed as

$$\sum_{1 \leqq i \leqq m} \lambda_{ij} a_i(c) = 0 \qquad (1 \leqq j \leqq m)\,,$$

which imply that $a_i(c) = 0$ $(1 \leqq i \leqq m)$.

LEMMA 3.5. *If $d > t$, $I_{s_0} \ni 1$ and $I \neq I_{s_0}$, then $a_i(p^t e_j) = 0$ $(t+1 \leqq j \leqq d)$ for each $i \in I - I_{s_0}$.*

Proof. Put $\zeta_v = \{vp^t - (v-1)p^{t-1}\}e_{t+1} \in \boldsymbol{Z}^d$ $(1 \leqq v \leqq p)$ and let $a_i(\zeta_p) = 0$ $(1 \leqq i \leqq m)$. Since $\Phi_{\zeta_v}(F_i(T_u)h_{1i}) = 0$ for $u \neq t+1$, by (2.9) we obtain

$$\begin{aligned}\Phi_{\zeta_v}\Big(\sum_{1 \leqq i \leqq m} F_i((\sigma_j - 1)X_i)h_{1i}\Big) &= \sum_{1 \leqq i \leqq m} \lambda_{ij}\Phi_{\zeta_v}(F_i(Z)h_{1i}) \\ &\quad + \sum_{i \in \tilde{I}} \lambda_{ij} b_{jt+1}\Phi_{\zeta_v}(F_i(T_{t+1})h_{1i}) \\ &= \sum_{i \in \tilde{I}} \lambda_{ij}\{a_i(\zeta_v) + b_{jt+1}a_i((v-1)(p^t - p^{t-1})e_{t+1})\} \\ &\quad + \sum_{i \in I - \tilde{I}} \lambda_{ij}\{a_i(\zeta_v) - a_i(\zeta_{v-1})\}\end{aligned}$$

where $\tilde{I} = \{i : \oplus_{u \neq t+1} kT_u \supseteqq \mathcal{A}(V^G \oplus W_i, H_i)\}$. But it follows from (3.4) that

$$a_i((v-1)(p^t - p^{t-1})e_{t+1}) = 0 \qquad (2 \leqq v \leqq p)\,.$$

Thus for $2 \leqq v \leqq p$ and $1 \leqq j \leqq m$ we must have

$$(0=)\Phi_{\zeta_v}(F_1((1-\sigma_j)X_1)^p) = \Phi_{\zeta_v}\Big(\sum_{1\leqq i\leqq m} F_i((\sigma_j-1)X_i)h_{1i}\Big)$$
$$= \sum_{i\in\tilde{I}} \lambda_{ij}a_i(\zeta_v) + \sum_{i\in I-\tilde{I}} \lambda_{ij}\{a_i(\zeta_v) - a_i(\zeta_{v-1})\}\ ,$$

which shows $a_i(p^te_{t+1})=0$ for $i\in I-\tilde{I}$. Further let i_0 be an element of $(I-I_{s_0})\cap\tilde{I}$ if it is non-empty. We may suppose $\oplus_{u\neq t+2}kT_u \not\supseteq \mathcal{A}(V^G\oplus W_{i_0}, H_{i_0})$ and set $\zeta'_v = p^te_{t+1}+(v-1)(p^t-p^{t-1})e_{t+2}$ $(1\leqq v\leqq p)$. Clearly

$$\Phi_{\zeta'_v}\Big(\sum_{1\leqq i\leqq m} F_i((\sigma_j-1)X_i)h_{1i}\Big) = \sum_{1\leqq i\leqq m}\lambda_{ij}\Big\{\Phi_{\zeta'_v}(F_i(Z)h_{1i}) + \sum_{u=t+1,t+2} b_{ju}\Phi_{\zeta'_v}(F_i(T_u)h_{1i})\Big\}$$

for $2\leqq v\leqq p$. On the other hand (2.9) implies

$$\Phi_{\zeta'_v}(F_{i_0}(Z)h_{1i_0}) = a_{i_0}(\zeta'_v) - a_{i_0}(\zeta'_{v-1}) \qquad (2\leqq v\leqq p)$$

because $\Phi_{\zeta'_v}(F_i(T_u)h_{1i})$ $(u=t+1, t+2)$ are linear combinations of $a_i(c)$ such that $c=(0,\cdots,0,c_{t+1},\cdots,c_d)$ and $\|c\|=(v-1)(p^t-p^{t-1})$. But we see

$$\Phi_{\zeta'_v}\Big(\sum_{1\leqq i\leqq m} F_i((\sigma_j-1)X_i)h_{1i}\Big) = \Phi_{\zeta'_v}(F_1((1-\sigma_j)X_1)^p) = 0$$
$$(2\leqq v\leqq p;\ 1\leqq j\leqq m)\ ,$$

and hence this system requires

$$a_{i_0}(p^te_{t+1}) = a_{i_0}(\zeta'_1) = \cdots = a_{i_0}(\zeta'_p) = 0\ .$$

The remainder can be proved in the same way.

Now let s_0 be an integer such that $I_{s_0}\ni 1$ and put $\tau_j = \sigma_j\sigma_{j_0}^{n_j}$ $(1\leqq j\leqq m)$ where $j_0\in J_{s_0}$ and $n_j\in N$ satisfy $\lambda_{1j_0}\neq 0$ and $n_j\lambda_{1j_0} = -\lambda_{1j}$ respectively. According to (3.3)

$$\Phi_{p^te_i}(F_u((\sigma_j-1)X_u)h_{1u}) = \lambda_{uj}\Phi_{p^te_i}\Big(F_u\Big(Z+\sum_{1\leqq v\leqq d} b_{jv}T_v\Big)h_{1u}\Big) = \lambda_{uj}a_u(p^te_i)$$

for $2\leqq u\leqq m$, and therefore if $t+1\leqq i\leqq d$ we deduce from (3.5) that

$$(0=)\Phi_{p^te_i}(F_1((1-\sigma_j)X_1)^p) = \sum_{1\leqq u\leqq m}\Phi_{p^te_i}(F_u((\sigma_j-1)X_u)h_{1u})$$
$$= \lambda_{1j}\{a_1(p^te_i)+b_{ji}a_1(0)\} + \sum_{u\in I_{s_0}-\{1\}}\lambda_{uj}a_u(p^te_i)\ .$$

Since $[\lambda_{uv}]_{(u,v)\in I_{s_0}\times J_{s_0}}$ is a monomial matrix, these equations imply

$$a_j(p^te_i) = 0 \qquad (t+1\leqq i\leqq d;\ 2\leqq j\leqq m).$$

So we have

$$a_1(p^te_i) = -b_{ji}a_1(0) = b_{ji} \qquad (t+1\leqq i\leqq d)$$

for $1 \leqq j \leqq m$ with $\lambda_{1j} \neq 0$, and then it follows from the definition of τ_j that $(\tau_j - 1)X_1 \in \bigoplus_{1 \leqq i \leqq t} kT_i$ $(1 \leqq j \leqq m)$. By the identities $F_1(T_i) = 0$ $(1 \leqq i \leqq t)$ we can see

$$\begin{aligned}\tau_j(f_1) &= \tau_j(F_1)^p + \sum_{1 \leqq i \leqq m} \tau_j(F_i)h_{1i} \\ &= F_1^p + F_1 h_{11} + \sum_{2 \leqq i \leqq m} \tau_j(F_i)h_{1i} .\end{aligned}$$

Consequently we obtain

$$(0 =)(\tau_j - 1)f_1 = \sum_{2 \leqq i \leqq m} (c_{ij}F_i(Z) + g_{ij})h_{1i}$$

for some homogeneous polynomials g_{ij} in $k[W]$ where

$$c_{ij} = \frac{(\tau_j - 1)X_i \bmod W}{Z \bmod W} .$$

Then, because $F_i(Z) \equiv Z^{p^t} \bmod \langle W \rangle$, this system requires $h_{1i} = 0$ $(2 \leqq i \leqq m)$.

For $i \neq j$ we conclude that $h_{ij} = 0$. Hence G contains subgroups G_i $(i = 1, 2)$ which satisfy $k[V]^{G_1} = k[V^G][f_1, X_2, X_3, \cdots, X_m]$ and $k[V]^{G_2} = k[V^G][X_1, f_2, f_3, \cdots, f_m]$. The couple (V, G) has a decomposition $\{(V^G \oplus kX_1, G_1), (V^G \oplus \bigoplus_{2 \leqq i \leqq m} kX_i, G_2)\}$. We have just completed the proof of (3.2).

§ 4. Proof of Theorem 1.3

We begin with

PROPOSITION 4.1. *Let (V, G) be a quasi-homogeneous couple with* $\dim(V, G) \geqq 2$. *Suppose that $(V, G(W))$ decomposes to one dimensional subcouples for any proper subspace W of V^G with $G(W) \neq \{1\}$. If $k[V]^G$ is a polynomial ring, then (V, G) is decomposable.*

Proof. Since (V, G) is quasi-homogeneous, there is a subspace W of V^G with $\operatorname{codim}_{V^G} W = 1$ such that $G(W) = \{1\}$ or $(V, G(W))$ is a homogeneous subcouple which satisfies $\dim(V, G(W)) = \dim(V, G) = m$. Clearly (V, G) is decomposable if $G(W)$ is trivial. Hence we suppose that $(V, G(W))$ decomposes to one dimensional subcouples $(V^G \oplus W_i, H_i)$ $(1 \leqq i \leqq m)$ with $|H_i| = p^t$. Denote by X_i a generator of W_i and let r be the rank of the matrix $[(\sigma_j - 1)X_i \bmod W]_{(i,j)}$ where σ_j runs through all pseudo-reflections in $G - G(W)$. In the case of $r = m$ we have already shown that (V, G) is decomposable. We may assume that $r < m$ and that the submatrix $[(\sigma_j - 1)X_i \bmod W]_{1 \leqq i, j \leqq r}$ is non-singular.

Let $F_i(X_i)$ be the canonical $(V^G \oplus W_i, H_i)$-invariant on X_i. Further choose Z_j from V with $(1-\sigma_j)V = kZ_j$ and put $b_{ij} = Z_j^{-1}(\sigma_j - 1)X_i$. Since $\mathscr{Q}(V, G(W))$ is homogeneous, by (2.8) we see $\mathscr{Q}(V,G) = k[\overline{X}_1^{p^{t+1}}, \cdots, \overline{X}_r^{p^{t+1}}, g_{r+1}, \cdots, g_m]$ where $\overline{X}_i = X_i \bmod V^G$ and g_j $(r+1 \leqq j \leqq m)$ are expressed as

$$g_j = \overline{X}_j^{p^t} + \sum_{1\leqq i\leqq r} a_{ij}\overline{X}_i^{p^t}$$

for some $a_{ij} \in k$. From this the polynomials

$$F_j(X_j) + \sum_{1\leqq i\leqq r} a_{ij}F_i(X_i) \qquad (r+1 \leqq j \leqq m)$$

belong to a regular system of homogeneous parameters of $k[V]^G$. Thus, for $r+1 \leqq j \leqq m$ and $1 \leqq u \leqq r$, we have

$$\begin{aligned} -b_{ju}F_j(Z_u) &= (1-\sigma_u)F_j(X_j) \\ &= \sum_{1\leqq i\leqq r} a_{ij}(\sigma_u - 1)F_i(X_i) \\ &= \sum_{1\leqq i\leqq r} b_{iu}a_{ij}F_i(Z_u)\,, \end{aligned}$$

which implies that if $a_{ij} \neq 0$

$$F_i(Z) = F_j(Z) \qquad (1 \leqq i \leqq r;\, r+1 \leqq j \leqq m)$$

where Z denotes a variable. Obviously this requires $\mathscr{A}(V^H \oplus W_i, H_i) = \mathscr{A}(V^H \oplus W_j, H_j)$. Define $\theta \in GL(V)$ to satisfy that

$$\theta(X_j) = X_j + \sum_{1\leqq i\leqq r} a_{ij}X_i \qquad (r+1 \leqq j \leqq m)$$

and $V^{\langle\theta\rangle} \supseteqq \{X_i : 1 \leqq i \leqq r\} \cup V^G$. According to (2.10) θ is a $\{(V^G \oplus W_i, H_i) : 1 \leqq i \leqq m\}$-admissible transform and (V, H) decomposes to subcouples $(V^G \oplus \theta(W_i), H_i')$ $(1 \leqq i \leqq m)$ for some subgroups H_i' of H. Then (V, G) decomposes to $(V^G \oplus \oplus_{r+1\leqq j\leqq m} \theta(W_j), \oplus_{r+1\leqq j\leqq m} H_j')$ and $(V^G \oplus \oplus_{1\leqq j\leqq r} \theta(W_j), L)$ where L is the stabilizer of G at $\oplus_{r+1\leqq j\leqq m} \theta(W_j)$.

(4.2) Let $A_i = K[f_{i1}, f_{i2}, \cdots, f_{in}]$ $(i = 1, 2)$ be graded polynomial algebras with $\dim A_i = n$ over a field K where f_{ij} are homogeneous in A_i. Suppose that A_1 is contained in A_2 as a graded subalgebra. Then $A_1 = A_2$ if and only if

$$\prod_{1\leqq j\leqq n} \deg f_{1j} = \prod_{1\leqq j\leqq n} \deg f_{2j}\,.$$

$q(R)$ denotes the quotient field of an integral domain R.

LEMMA 4.3. *For any couple (V, G) we have the following inequality;*

$$[q(k[V/V^G]) : q(\mathcal{Q}(V, G))] \geqq |G|$$

and if the equality holds then $k[V]^G$ *is a polynomial ring.*

Proof. We prove this by induction on $|G|$. Let W be a subspace of V^G such that $\operatorname{codim}_{V^G} W = 1$ and $W \not\supseteq \mathscr{A}(V, G)$. Then $H = G(W)$ is a proper subgroup of G. By the induction hypothesis we have

$$[q(k[V]/\langle W\rangle) : q(k[V]^H/\langle W\rangle^H)] \geqq |H|$$

and if the equality holds $k[V]^H$ is a polynomial ring. Putting

$$S = (\bar{k}[\bar{k} \otimes_k V]^H/(\langle \bar{k} \otimes_k W\rangle_{\bar{k}[\bar{k}\otimes_k V]})^H)^{G/H},$$

as in the proof of (2.3), we can show that $S_{\mathfrak{M}_1} \cong S_{\mathfrak{M}_2}$ for any maximal ideals $\mathfrak{M}_i$ $(i = 1, 2)$ of S which contain the minimal prime ideal $((\langle \bar{k} \otimes_k V^G\rangle_{\bar{k}[\bar{k}\otimes_k V]})^H/(\langle \bar{k} \otimes_k W\rangle_{\bar{k}[\bar{k}\otimes_k V]})^H)^{G/H}$. On the other hand it follows easily from (2.3) that S is normal and hence S is a polynomial ring over $\bar{k}$. Since

$$\bar{k} \otimes_k (k[V]^H/\langle W\rangle^H)^{G/H} \cong S$$

as graded algebras defined over $\bar{k}$, $(k[V]^H/\langle W\rangle^H)^{G/H}$ is also a polynomial ring. Clearly $\mathcal{Q}(V, G)$ can be embedded in $(k[V]^H/\langle W\rangle^H)^{G/H}/(\langle V^G\rangle^H/\langle W\rangle^H)^{G/H}$ and so we have

$$[q(k[V/V^G]) : q(\mathcal{Q}(V, G))] \geqq |G| .$$

Now suppose that the equality of (4.3) holds and then we deduce from this

$$[q(k[V]/\langle W\rangle) : q(k[V]^H/\langle W\rangle^H)] = |H| .$$

Therefore $k[V]^H$ is a polynomial ring. Moreover by the equality of (4.3) and (2.3) we see that the canonical map

$$\mathcal{Q}(V, G) \longrightarrow (k[V]^H/\langle W\rangle^H)^{G/H}/(\langle V^G\rangle^H/\langle W\rangle^H)^{G/H}$$

is an isomorphism and that there is an $(n + 1)$-dimensional graded polynomial subalgebra $k[f_1, f_2, \cdots, f_{n+1}]$ of $k[V]^G/\langle W\rangle^G$ with

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

Here n denotes the dimension of (V, G) and f_i $(1 \leqq i \leqq n + 1)$ are homogeneous elements in $k[V]/\langle W\rangle$. Then, by (4.2), we must have $(k[V]^H/\langle W\rangle^H])^{G/H} = k[V]^G/\langle W\rangle^G$, because $(k[V]^H/\langle W\rangle^H)^{G/H}$ is a polynomial ring which contains $k[V]^G/\langle W\rangle^G$ as a graded subalgebra.

Further if $\dim W \geqq 2$ let W' be a subspace of W with $\operatorname{codim}_W W' = 1$ and put $H' = G(W')(=H(W'))$. Since $k[V]^H$ is a polynomial ring, by (2.6) $k[V]^{H'}$ is also a polynomial ring. Therefore we get the commutative diagram

$$\begin{array}{ccccc} k[V]^H/\langle W'\rangle^H & \longrightarrow & k[V]^H/\langle W\rangle^H & \longrightarrow & 0 \\ \| & & \wr\downarrow & & \\ (k[V]^{H'}/\langle W'\rangle^{H'})^{H/H'} & \longrightarrow & (k[V]^{H'}/\langle W'\rangle^{H'})^{H/H'}/(\langle W\rangle^{H'}/\langle W'\rangle^{H'})^{H/H'} & \longrightarrow & 0 \end{array}$$

of kG/H-modules with exact rows. From $(k[V]^H/\langle W\rangle^H)^{G/H} = k[V]^G/\langle W\rangle^G$ the sequence

$$(k[V]^H/\langle W'\rangle^H)^{G/H} \longrightarrow (k[V]^H/\langle W\rangle^H)^{G/H} \longrightarrow 0$$

is exact. Then $(k[V]^{H'}/\langle W'\rangle^{H'})^{G/H'}$ is a polynomial ring which contains $k[V]^G/\langle W'\rangle^G$, because $(\langle W\rangle^{H'}/\langle W'\rangle^{H'})^{G/H'}$ is principal. Hence we deduce similarly from the equality of (4.3) and (2.3) that $k[V]^G/\langle W'\rangle^G = (k[V]^{H'}/\langle W'\rangle^{H'})^{G/H'}$.

If necessary we can continue this procedure. Consequently $k[V]^G/\langle \tilde{W}\rangle^G$ is a polynomial ring for a one dimensional subspace $\tilde{W}$ of V^G. The assertion follows immediately from this.

By the use of (4.1) we establish

THEOREM 4.4. *Let (V, G) be an indecomposable couple. Then $k[V]^G$ is a polynomial ring if and only if* $\dim(V, G) = 1$.

Proof. It suffices to prove the "only if" part. Let $\mathscr{C}$ denote the set of all indecomposable couples (V_0, G_0) with $\dim(V_0, G_0) \geqq 2$ such that $k[V_0]^{G_0}$ are polynomial rings. Assume that $\mathscr{C}$ is non-empty and choose an element (V, G) from $\mathscr{C}$ which is minimal with respect to the lexicographical preorder of $\mathscr{C}$ defined by the value $(\dim(V_0, G_0), \dim V_0)$ for $(V_0, G_0) \in \mathscr{C}$. From (4.1) the couple (V, G) is not quasi-homogeneous. Let W be a subspace of V^G with $\operatorname{codim}_{V^G} W = 1$ and put $H = G(W)$ and $u = \dim V^H/V^G$ respectively. Then the kH-module V defines a couple (V, H) and by (2.6) $k[V]^H$ is a polynomial ring. Obviously V is decomposable as a kH-module, and hence (V, H) decomposes to one dimensional subcouples $(V^H \oplus W_i, H_i)$ $(u+1 \leqq i \leqq m)$ where $m = \dim(V, G)$, since (V, G) is minimal in $\mathscr{C}$. If (V, H) is not homogeneous, we may suppose that

$$|H_{u+1}| \leqq \cdots \leqq |H_v| < |H_{v+1}| = \cdots = |H_m|$$

for some $v < m$. Otherwise set $v = u$ (it should be noted that $u > 0$ in this case).

Let $U = V^H \oplus \oplus_{u+1 \leqq i \leqq v} W_i$ (the empty direct sum is regarded as $\{0\}$) and denote by G' the stabilizer of G at U. We can choose homogeneous polynomials $f_i \in k[V]$ $(1 \leqq i \leqq m)$ such that $f_i \in k[U]$ $(1 \leqq i \leqq v)$ and $k[V]^G = k[V^G][f_1, \cdots, f_m]$, calculating a regular system of parameters of $\mathcal{Q}(V, G)$ through $k[V]^H/\langle W\rangle^H$ as in the proof of (2.7). Because $k[V]^G$ is contained in $k[U][f_{v+1}, \cdots, f_m]$, there is a subgroup $\tilde{G}$ of G with $k[V]^{\tilde{G}} = k[U][f_{v+1}, \cdots, f_m]$. Clearly $\tilde{G} = G'$ and the kG'-module V is decomposable. Therefore, from the minimality of (V, G), the couple (V, G') decomposes to one dimensional subcouples $(V^{G'} \oplus W'_i, G'_i)$ $(v + 1 \leqq i \leqq m)$.

We have

$$[q(k[U/V^G]): q(\mathcal{Q}(U, G/G'))] = |G/G'|$$

since $f_i \in k[U]^{G/G'}$ $(1 \leqq i \leqq v)$ and G/G' acts faithfully on U. By (4.3) $k[U]^{G/G'}$ is a polynomial ring and so $(U, G/G')$ decomposes to one dimensional subcouples $(U^{G/G'} \oplus W'_i, G'_i)$ $(1 \leqq i \leqq v)$. It should be noted that $V^{G'} = U$ and $U^{G/G'} = V^G$.

Let X_i $(1 \leqq i \leqq m)$ denote a generator of W'_i and put $\bar{G} = G/G'$ and $p^r = [\bar{G}: \oplus_{u+1 \leqq i \leqq v} H_i]$ respectively. Because $k[U]^{\bar{G}} = k[V^G][f_1, \cdots, f_v]$ by (4.2), we deduce from the computation of $\mathcal{Q}(V, G)$ (cf. (2.7)) that there exist pseudo-reflections σ_i $(1 \leqq i \leqq r)$ in $G - H$ such that the column vectors $[(\sigma_j - 1)X_i \bmod W]_{1 \leqq i \leqq v}$ $(1 \leqq j \leqq r)$ are linearly independent. Then $\bar{G}(W) \cap \oplus_{1 \leqq i \leqq r} \langle \sigma_i \bmod G' \rangle = \{1\}$ and hence we see that $\bar{G}(W) = \oplus_{u+1 \leqq i \leqq v} H_i$. Putting

$$H'_i = \begin{cases} G'_i \cap \bigoplus_{u+1 \leqq j \leqq v} H_j & (1 \leqq i \leqq v) \\ G'_i \cap H & (v + 1 \leqq i \leqq m)\,, \end{cases}$$

we obtain another decomposition

$$\{(V^H \oplus W'_i, H'_i): 1 \leqq i \leqq m \text{ with } H'_i \neq \{1\}\}$$

of (V, H). Since $\{i: H'_i = \{1\}\} \subseteqq \{1, 2, \cdots, v\}$, it may be assumed that $H'_i = \{1\}$ $(1 \leqq i \leqq u)$.

Let $F_i(X_i) = X_i$ $(1 \leqq i \leqq u)$ and for $u + 1 \leqq i \leqq m$ (resp. $1 \leqq i \leqq m$) let $F_i(X_i)$ (resp. $g_i(X_i)$) be the canonical $(V^H \oplus W'_i, H'_i)$-invariant (resp. $(V^G \oplus W'_i, G'_i)$-invariant) on X. Assume that $G'_{i_0} = H'_{i_0}$ for some $u + 1 \leqq i_0 \leqq v$. Then (V, G) decomposes to $(V^G \oplus W'_{i_0}, H'_{i_0})$ and $(V^G \oplus \oplus_{i \neq i_0} W'_i, L)$ where L is the stabilizer of G at W'_{i_0}, and hence we must have $|G'_i/H'_i|$

$= p$ for all $u+1 \leqq i \leqq v$. Because $k[V]^G$ is contained in

$$k[V^G \oplus \bigoplus_{\substack{i \neq j \\ 1 \leqq i \leqq v}} W_i'][g_j, f_{v+1}, \cdots, f_m]\ ,$$

there are pseudo-reflections τ_j $(1 \leqq j \leqq v)$ in $G - H$ which satisfy the following condition; for $1 \leqq i \leqq v$ $V^{\langle\tau_j\rangle} \supseteqq W_i'$ if and only if $i \neq j$. We may suppose that $V^{\langle\tau_i\rangle} \supseteqq W_j'$ $(1 \leqq i \leqq u; v+1 \leqq j \leqq m)$ and $\mathscr{A}(V^H \oplus W_j', H_j') \not\supseteq \mathscr{A}(V^H \oplus W_i', H_i')$ $(u+1 \leqq i \leqq v; v+1 \leqq j \leqq m)$, applying a $\{(V^H \oplus W_i', H_i'): u+1 \leqq i \leqq m\}$-admissible transform on V.

Clearly we may assume that $\deg f_i = \deg g_i$ $(v+1 \leqq i \leqq m)$ and

$$\deg f_{v+1} = \deg f_{v+2} = \cdots = \deg f_y < \deg f_{y+1} = \cdots = \deg f_m$$

for some y with $v+1 \leqq y \leqq m$. Further $f_i - g_i$ $(v+1 \leqq i \leqq y)$ can be regarded as a polynomial h_i in $k[U]$, replacing f_i with linear combinations of them. We deduce from (3.1) that

$$h_i = \sum_{1 \leqq j \leqq v} F_j h_{ij} \ (v+1 \leqq i \leqq y)$$

for some homogeneous polynomials h_{ij} in $k[V^G]$, since $(\tau_j - 1)g_i \in k[V^G]$ $(v+1 \leqq i \leqq y; 1 \leqq j \leqq v)$ and

$$k[U]^{\underset{1 \leqq i \leqq v}{\oplus} H_i'} = \bigoplus_{\substack{0 \leqq i_j < p \\ 1 \leqq j \leqq v}} k[V^G][g_1, g_2, \cdots, g_v] F_1^{i_1} F_2^{i_2} \cdots F_v^{i_v}\ .$$

Assume that $h_{i_0 j_0} \neq 0$ and let Z_{j_0} be an element of V with $(1 - \tau_{j_0})V = kZ_{j_0}$. Then it follows from $\tau_{j_0}(f_{i_0}) = f_{i_0}$ that

$$k^* h_{i_0 j_0} F_{j_0}(Z_{j_0}) \ni \frac{(1 - \tau_{j_0})X_{i_0}}{Z_{i_0}} g_{i_0}(Z_{j_0})\ .$$

So we have $u+1 \leqq j_0 \leqq v$ and $\mathscr{A}(V^H \oplus W_{i_0}', H_{i_0}') \not\supseteq \mathscr{A}(V^H \oplus W_{j_0}', H_{j_0}')$. Moreover we find a pseudo-reflection σ in $G_{i_0}' - H_{i_0}'$ because $F_{i_0} = g_{i_0}$ requires $\mathscr{A}(V^H \oplus W_{i_0}', H_{i_0}') \supseteqq \mathscr{A}(V^H \oplus W_{j_0}', H_{j_0}')$, and choose $Z_\sigma \in V$ such that $(1-\sigma)V = kZ_\sigma$ and $Z_{j_0} \equiv Z_\sigma \bmod W$. Let $\{T_i : 1 \leqq i \leqq t\}$ be a k-basis of $\mathscr{A}(V^H \oplus W_{i_0}', H_{i_0}')$ and select $T_j \in V$ $(t+1 \leqq j \leqq d)$ to satisfy $W = \oplus_{1 \leqq i \leqq d} kT_i$ and $\oplus_{1 \leqq i \leqq d-1} kT_i \not\supseteq \mathscr{A}(V^H \oplus W_{j_0}', H_{j_0}')$. Express Z_{j_0} as

$$Z_{j_0} = Z + \sum_{1 \leqq i \leqq d} a_i T_i$$

for $a_i \in k$ $(1 \leqq i \leqq d)$ and set $R = k[T_1, \cdots, T_{d-1}, Z]$. If $a_d = 0$, by (2.9) we have $(1 - \tau_{j_0})F_{j_0} \notin R$ and $g_{i_0}(Z_{j_0}) \in R$. This implies that $a_d \neq 0$. Since $g_{i_0}(Z_\sigma) = g_{i_0}(Z_j) = 0$ $(1 \leqq j \leqq t)$, we see

$$g_{i_0}(Z_{j_0}) = \sum_{t+1 \leqq j \leqq d} a_j g_{i_0}(T_j) .$$

Then $g_{i_0}(Z_{j_0})$ is a monic polynomial of T_d in $R[T_d]$, but from (2.9) the leading coefficient of $F_{j_0}(Z_{j_0})$ as a polynomial of T_d is a non-unit in R, which is a contradiction. Therefore we must have $f_i = g_i$ $(v+1 \leqq i \leqq y)$.

In the case of $y = m$ it follows that $k[V]^G = k[V^G][g_1, \cdots, g_m]$ and this requires that (V, G) is decomposable. Hence we obtain $y < m$. Because $G'_i = H'_i$ $(v+1 \leqq i \leqq y)$, the couple (V, G) decomposes to $(V^G \oplus \oplus_{v+1 \leqq i \leqq y} W'_i, \oplus_{v+1 \leqq i \leqq y} H'_i)$ and $(V^G \oplus \oplus_{1 \leqq i \leqq v} W'_i \oplus \oplus_{y+1 \leqq i \leqq m} W'_i, K)$ where K denotes the stabilizer of G at the set $\oplus_{v+1 \leqq i \leqq y} W'_i$. This conflicts with the selection of (V, G). Thus the proof is completed.

Now (1.3) can be reduced to (4.4) by (2.1), (2.2) and (2.4).

References

[1] N. Bourbaki, Groupes et algèbres de Lie, Ch. 4, 5 et 6, Hermann, Paris, 1968.
[2] C. Chevalley, Invariants of finite groups generated by reflections, Amer. J. Math., **77** (1955), 778–782.
[3] J.-P. Serre, Groupes finis d'automorphismes d'anneaux locaux réguliers, Colloq. d'Alg. E.N.S., (1967).

Keio University
Present Address:
Department of Mathematics
Tokyo Metropolitan University
Fukasawa, Setagaya-ku, Tokyo 158, Japan