TSUKUBA J. MATH.
Vol. 3, No. 1 (1979), 109–122

INVARIANTS OF FINITE GROUPS GENERATED BY PSEUDO-REFLECTIONS IN POSITIVE CHARACTERISTIC

By
Haruhisa NAKAJIMA

Introduction

Let R be a commutative ring, and let V be a finitely generated free R-module. Let $R[V]$ be a polynomial ring over R associated with V. Then a finite subgroup G of $GL(V)$ acts naturally on $R[V]$. We denote by $R[V]^G$ the ring of invariants of $R[V]$ under the action of G.

Let $R=k$ be a field and suppose that $|G|$ is a unit of k. It is known ([4], [9], [3], [8]) that $k[V]^G$ is a polynomial ring if and only if G is generated by pseudo-reflections in $GL(V)$.

But, in the case where $|G|\equiv 0$ *mod char*(k), there are only the following results:

(1) L. E. Dickson [5]; $\boldsymbol{F}_q[T_1, \cdots, T_n]^{GL(n,q)}$ and $\boldsymbol{F}_q[T_1, \cdots, T_n]^{SL(n,q)}$ are polynomial rings, where $\boldsymbol{F}_q$ is the finite field of q elements.

(2) M.-J. Bertin [1]; $\boldsymbol{F}_q[T_1, \cdots, T_n]^{Unip(n,q)}$ is a polynomial ring, where

$$Unip(n,q)=\left\{\sigma\in GL(n,q):\ \sigma=\begin{bmatrix}1 & & 0\\ & \ddots & \\ * & & 1\end{bmatrix}\right\}.$$

(3) J.-P. Serre [8]; (i) If $k[V]^G$ is a polynomial ring, then G is generated by pseudo-reflections in $GL(V)$. (ii) $\boldsymbol{F}_q[T_1, T_2, T_3, T_4]^{O_4^+(\boldsymbol{F}_q)}$ is not a polynomial ring, where $O_4^+(\boldsymbol{F}_q)$ is the orthogonal group and $char(\boldsymbol{F}_q)\neq 2$.

The purpose of this paper is to determine finite irreducible subgroups G of $GL(V)$ such that $k[V]^G$ are polynomial rings in the case where $|G|\equiv 0$ *mod char*(k). Let V be an n-dimensional vector space over a finite field k of characteristic p and let G be a subgroup of $GL(V)$. Then our results are the following

[I] *If G is a transitive imprimitive group generated by pseudo-reflections, then $k[V]^G$ is a polynomial ring.*

[II] *Suppose that $p\neq 2$, $n\geqq 3$ and G is an irreducible group generated by transvections. Then $k[V]^G$ is a polynomial ring if and only if G is conjugate in $GL(V)$*

Received June 2, 1978. Revised December 25, 1978

to $SL(n, q)$.

[III] *Suppose that* $p \neq 2$ *and* V *is a faithful linear representation of least degree of the symmetric group* S_m *of degree* m *with* $m \geqq 7$. *Then* $k[V]^{S_m}$ *is a polynomial ring if and only if* $(m, p)=1$ *and all transpositions of* S_m *are represented by reflections in* $GL(V)$.

[IV] *Let* F *be a subfield of* k *and let* $O_n(F)$ *be the orthogonal group of dimension* n *over* F. *Suppose that* G *is a subgroup of* $O_n(F)$ *which contains the commutator subgroup* $\Omega_n(F)$ *of* $O_n(F)$. *If* $n \geqq 4$, *then* $k[V]^G$ *is not a polynomial ring.*

Let $G \subseteqq GL(V)$ be an irreducible primitive group and let $p \neq 2$. If G is generated by transvections, G is called a transvection group. Transvection groups are classified by A. E. Zalesskii and V. N. Serezkin [11]. This result will be used in the proof of [II]. On the other hand G is called a reflection group if G is a group generated by reflections which contains no transvections. By using the classification stated in V. N. Serezkin [7], we can determine all reflection groups G such that $k[V]^G$ are polynomial rings under the assumption of $n \geqq 4$, $p > 7$. For convenience we will describe their results in § 1.

§ 1. Preliminaries

Let V be a vector space over a field k. According to [2], an element $\sigma \in GL(V)$ is called a pseudo-reflection in V if $\dim V_\sigma \leqq 1$ where $V_\sigma = (1-\sigma)V$.

On the other hand an automorphism σ of an integral domain R is called a generalized reflection in R if $(\sigma-1)R \subseteqq \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of R of height 1. For a subgroup G of $Aut(R)$ and a prime ideal $\mathfrak{p}$ of R, we put $D_G(\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ (resp. $I_G(\mathfrak{p}) = \{\sigma \in G : (\sigma-1)R \subseteqq \mathfrak{p}\}$) which is called the decomposition group of G at $\mathfrak{p}$ (resp. the inertia group of G at $\mathfrak{p}$).

Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a graded algebra over R_0 with a graduation $\{R_i\}$. We define that

$$Aut_{gr}(R) = \{\sigma \in Aut(R) : \sigma \text{ preserves the graduation of } R\},$$

$$Aut_{R_0\text{-}gr}(R) = \{\sigma \in Aut_{gr}(R) : \sigma \text{ acts trivially on } R_0\},$$

$$R_+ = \bigoplus_{i>0} R_i .$$

THEOREM 1.1. ([8]) *Let* R *be a regular local ring with the residue class field* k. *Let* G *be a finite subgroup of* $Aut(R)$ *such that* $|G| \cdot 1_R \in U(R)$ *and* $k^G = k$, *where* $U(R)$ *denotes the unit group of* R. *Then* R^G *is a regular local ring if and only if* G *is generated by generalized reflections.*

The following lemma is well known.

LEMMA 1.2. *Let R be a noetherian graded algebra over a field k. Then the following conditions are equivalent*:

(1) *R is a graded polynomial algebra over k.*

(2) *R_{R_+} is a regular local ring.*

For an element σ of $Aut(R)$ and a σ-stable prime ideal $\mathfrak{p}$, σ induces an element of $Aut(R_{\mathfrak{p}})$ which is denoted by the same symbol σ. Let $R=\bigoplus_{i=0}^{\infty} R_i$ be a noetherian graded polynomial algebra over a field $R_0=k$. Then, for $\sigma\in Aut_{k\text{-}gr}(R)$, σ is a generalized reflection in R if and only if σ is so in R_{R_+}. Therefore, from (1.1), we obtain

COROLLARY 1.3. *Let $R=\bigoplus_{i=0}^{\infty} R_i$ be a noetherian graded polynomial algebra over a field $R_0=k$, and let G be a finite subgroup of $Aut_{k\text{-}gr}(R)$ such that $|G|\cdot 1_k\in U(k)$. Then R^G is a graded polynomial algebra over k if and only if G is generated by generalized reflections.*

LEMMA 1.4. (e.g. [2]) *Suppose that $R=k[T_1, \cdots, T_n]$ is a polynomial ring over an algebraically closed field k and that G is a finite subgroup of $GL_n(k)$. If R^G is a polynomial ring, then $R^{D_G(\mathfrak{m})}$ is a polynomial ring for any maximal ideal $\mathfrak{m}$ of R and $D_G(\mathfrak{m})$ is generated by pseudo-reflections.*

PROOF. $dim({R_{\mathfrak{m}}}^{D_G(\mathfrak{m})})=dim((R^G)_{\mathfrak{m}\cap R^G})$ and ${R_{\mathfrak{m}}}^{D_G(\mathfrak{m})}$ is unramified over $(R^G)_{\mathfrak{m}\cap R^G}$. Hence ${R_{\mathfrak{m}}}^{D_G(\mathfrak{m})}$ is a regular local ring. Since $\mathfrak{m}$ is $D_G(\mathfrak{m})$-stable,

$$ {R_{\mathfrak{m}}}^{D_G(\mathfrak{m})}=(R^{D_G(\mathfrak{m})})_{\mathfrak{m}\cap R^{D_G(\mathfrak{m})}} . $$

On the other hand there exist elements $a_i\in k$ $(1\leqq i\leqq n)$ such that $\mathfrak{m}=(T_1-a_1, \cdots, T_n-a_n)$. Put $X_i=T_i-a_i$ $(1\leqq i\leqq n)$ and regard $R=k[X_1, \cdots, X_n]$ as a graded algebra by $deg X_i=1$. Then $D_G(\mathfrak{m})\subseteqq Aut_{k\text{-}gr}(R)$ and $R_+=\mathfrak{m}$. Therefore $S=R^{D_G(\mathfrak{m})}$ is a graded subalgebra of R and $S_+=\mathfrak{m}\cap R^{D_G(\mathfrak{m})}$. Since S_{S_+} is a regular local ring, S is a polynomial ring over k by (1.2). Hence $D_G(\mathfrak{m})$ is generated by pseudo-reflections.

From here to the end of this section, we assume that V is an n-dimensional vector space over a finite field k of characteristic $p\neq 2$. A pseudo-reflection $\sigma\neq 1$ is called a transvection if $\sigma|V_\sigma=1$ and a reflection if $\sigma|V_\sigma=-1$. Let G be a subgroup of $GL(V)$. Then we use the following notation:

$$ P(G)=\{\sigma\in G: \sigma \text{ is a pseudo-reflection}\}, $$

$$ T(G)=\{\sigma\in G: \sigma \text{ is a transvection}\}, $$

$$ R(G)=\{\sigma\in G: \sigma \text{ is a reflection}\}. $$

A. E. Zalesskii and V. N. Serezkin obtained the following result which gives the classification of transvection groups.

THEOREM 1.6. ([11]) *Suppose that* $G \subsetneqq GL(V)$ $(n \geqq 2)$ *is a transvection group. Then* G *is conjugate in* $GL(V)$ *to one of the groups* $SL(n, q)$, $Sp(n, q)$ *or* $SU(n, q)$, *except for the case where* $G \cong SL(2, 5)$, $G \subsetneqq SL(2, 3^2)$.

Recently V. N. Serezkin obtained the following

THEOREM 1.7. ([6], [7]) *Suppose* $n > 3$, $p > 5$. *Let* $G \subsetneqq GL(V)$ *be a reflection group. Then* G *is conjugate in* $GL(V)$ *to one of the groups in the following list*:

(1) *The orthogonal groups* $O_{2m+1}(F)$, $O^{\pm}_{2m}(F)$, *where* F *is a subfield of* k *and* $n = 2m+1$, $2m$ *respectively, or the groups* $x \cdot \Omega$, *where* $x \in R(O_n(F))$ *and* Ω *is the commutator subgroup of the orthogonal group* $O_n(F)$.

(2) *The symmetric groups* S_{n+1} *where* $n+1 \not\equiv 0$ *mod* p, *and* S_{n+2} *where* $n+2 \equiv 0$ *mod* p.

(3) *The nine exceptional groups, namely,*

$W(F_4)$, $W(N_4)$, $EW(N_4)$, $W(H_4)$ *where* $n=4$; $W(K_5)$ *where* $n=5$;
$W(K_6)$, $W(E_6)$ *where* $n=6$; $W(E_7)$ *where* $n=7$; $W(E_8)$ *where* $n=8$.

However the complete proof of this result has not been published yet.

For a field k of characteristic $p > 7$, the orders of the groups in part (3) of (1.7) are units in k.

§ 2. Monomial groups

Let V be a finitely generated free module over a commutative ring R. A subgroup G of $GL(V)$ is said to be monomial if G has a monomial form on some R-basis of V ([12], §43). For a field k, if $G \subsetneqq GL_n(k)$ is a finite transitive imprimitive group generated by pseudo-reflections, then G is a monomial group.

In this section, we use the following notation.

NOTATION 2.1. *Let* R *be an integral domain and* k *be the quotient field of* R. *Put*

$$\Pi_n(R) = \{\sigma \in GL_n(R) : \sigma \text{ is a permutation matrix}\},$$

$$D_n(R) = \{\sigma \in GL_n(R) : \sigma \text{ is diagonal}\}.$$

For a finite subgroup G *of* $GL_n(R)$ *of monomial form, the sequence* $1 \to D(G) \to G \xrightarrow{\Delta} \Pi_n(R)$ *is exact, where* $\Delta : G \to \Pi_n(R)$ *is the canonical homomorphism and* $D(G) = D_n(R) \cap G$. *Let*

$$\tilde{P}(G)=\{\sigma\in G:\ \sigma \text{ is a pseudo-reflection in } GL_n(k)\}.$$

We identify S_n *with* $\Pi_n(R)$.

LEMMA 2.2. *Let* $G\subseteqq GL_n(R)$ *be a finite subgroup of monomial form generated by pseudo-reflections in* $GL_n(k)$. *Assume that the following conditions are satisfied*:

(1) *The sequence* $1\to D(G)\to G\to\Pi_n(R)\to 1$ *is exact and* $\Pi_n(R)$ *is contained in* G.

(2) $\tilde{P}(D(G))=\{E_n\}$.

Then $R[T_1,\cdots,T_n]^G$ *is a polynomial ring.*

PROOF. For $r\in\tilde{P}(G)-\{E_n\}$, there exists $\tau_r\in\Pi_n(R)$ such that $\tau_r^{-1}\Delta(r)r\tau_r\in H=diag[D_2(R),1_{n-2}]$ where $diag[D_2(R),1_{n-2}]=\{diag[\sigma,1_{n-2}]:\ \sigma\in D_2(R)\}$. For matrices $A,B,C,\cdots$, $diag[A,B,C,\cdots]$ means the block diagonal matrix defined canonically. Put $L=\{\tau_r^{-1}\Delta(r)r\tau_r:\ r\in\tilde{P}(G)-\{E_n\}\}\cup\{E_n\}$. Then L is a subgroup of H and there is a monomorphism from L into $U(R)$. Hence L is generated by $\sigma_1=diag[a,a^{-1},1_{n-2}]$. Let $\sigma_2=diag[a,1,a^{-1},1_{n-3}],\cdots,\sigma_{n-1}=diag[a,1_{n-2},a^{-1}]$ and put $m=|\langle a\rangle|$. It is easy to show that $D(G)=\langle\sigma_1,\sigma_2,\cdots,\sigma_{n-1}\rangle$. Since any monomial of $R[T_1,\cdots,T_n]$ is a semi-invariant of $D(G)$, we have $R[T_1,\cdots,T_n]^{D(G)}=R[T_1^m,\cdots,T_n^m,\prod_{i=1}^n T_i]$. Let $S=R[T_1,\cdots,T_n]^{D(G)}$, $\tilde{S}=R[T_1^m,\cdots,T_n^m]$, $U=\prod_{i=1}^n T_i$, $X_i=T_i^m(1\leqq i\leqq n)$. Then $S=\tilde{S}\oplus\tilde{S}U\oplus\cdots\oplus\tilde{S}U^{m-1}$ and $G/D(G)$ acts on S as permutations of $\{X_1,\cdots,X_n\}$. Let U_i $(1\leqq i\leqq n-1)$ be the fundamental symmetric polynomial of degree i in $R[X_1,\cdots,X_n]$. Then we must have $R[T_1,\cdots,T_n]^G=R[U_1,\cdots,U_{n-1},U]$.

LEMMA 2.3. *Let* $V=\bigoplus_{i=1}^n RY_i$ *be a free* R*-module and let* G *be a finite subgroup of* $GL(V)$ *generated by the set* $\tilde{P}(G)$ *such that* G *has a monomial form on the basis* $\{Y_1,\cdots,Y_n\}$. *Then there is an* R*-basis* $\{X_1,\cdots,X_n\}$ *of* V *such that the following conditions are satisfied*:

(1) G *has a monomial form on the basis* $\{X_1,\cdots,X_n\}$.

We regard G *as a subgroup of* $GL_n(R)$ *afforded by* $\{X_1,\cdots,X_n\}$. *Let* $\Delta:G\to\Pi_n(R)$ *be the canonical homomorphism.*

(2) *There exists a canonical isomorphism* $H\cong\Pi_{n_1}(R)\times\cdots\times\Pi_{n_s}(R)$, *where* $H=Im(\Delta)$ *and* $\sum_{i=1}^s n_i=n$.

(3) H *is contained in* G.

PROOF. We identify G with the image of the matrix representation of G afforded by the R-basis $\{Y_1,\cdots,Y_n\}$. Let H' be the image of the canonical homomorphism $\Delta':G\to\Pi_n(R)$. Since G is generated by the set $\tilde{P}(G)$, we may assume that $H'=H_1\times\cdots\times H_s$ where

$$H_1=diag[\Pi_{n_1}(R), 1_{n-n_1}], \quad H_2=diag[1_{n_1}, \Pi_{n_2}(R), 1_{n-n_1-n_2}],$$
$$\cdots, H_s=diag[1_{n-n_s}, \Pi_{n_s}(R)].$$

Since $\Delta'^{-1}((i, i+1))\cap\tilde{P}(G)\neq\phi$ $(1\leqq i\leqq n-1)$, we can choose the following elements:

$$\Delta'^{-1}((1, 2))\cap\tilde{P}(G)\ni\sigma_1^{(1)}, \cdots, \Delta'^{-1}((1, n_1))\cap\tilde{P}(G)\ni\sigma_{n_1-1}^{(1)},$$
$$\Delta'^{-1}((n_1+1, n_1+2))\cap\tilde{P}(G)\ni\sigma_1^{(2)}, \cdots,$$
$$\Delta'^{-1}((n_1+1, n_1+n_2))\cap\tilde{P}(G)\ni\sigma_{n_2-1}^{(2)},$$

....

$$\Delta'^{-1}\left(\left(\sum_{i=1}^{s-1} n_i+1, \sum_{i=1}^{s-1} n_i+2\right)\right)\cap\tilde{P}(G)\ni\sigma_1^{(s)}, \cdots,$$
$$\Delta'^{-1}\left(\left(\sum_{i=1}^{s-1} n_i+1, n\right)\right)\cap\tilde{P}(G)\ni\sigma_{n_s-1}^{(s)}.$$

Put

$$X_1=Y_1, X_2=Y_1^{\sigma_1^{(1)}}, \cdots, X_{n_1}=Y_1^{\sigma_{n_1-1}^{(1)}},$$
$$X_{n_1+1}=Y_{n_1+1}, X_{n_1+2}=Y_{n_1+1}^{\sigma_1^{(2)}}, \cdots, X_{n_1+n_2}=Y_{n_1+1}^{\sigma_{n_2-1}^{(2)}},$$

....

$$X_{\sum_{i=1}^{s-1} n_i+1}=Y_{\sum_{i=1}^{s-1} n_i+1}, \cdots, X_n=Y_{\sum_{i=1}^{s-1} n_i+1}^{\sigma_{n_s-1}^{(s)}}.$$

Then $\{X_1, \cdots, X_n\}$ is the R-basis of V such that the conditions stated in this lemma are satisfied.

THEOREM 2.4. *Let G be a finite monomial subgroup of $GL_n(R)$ generated by pseudo-reflections in $GL_n(k)$. Then $R[T_1, \cdots, T_n]^G$ is a polynomial ring over R.*

PROOF. By (2.3), we may assume that G is indecomposable in $GL_n(R)$. Hence G contains the group $\Pi_n(R)$. Since $H=\langle\tilde{P}(D(G))\rangle$ is a normal subgroup of G, there is an integer m such that $R[T_1, \cdots, T_n]^H=R[T_1^m, \cdots, T_n^m]$. G/H acts R-linealy on $\sum_{i=1}^{n} RX_i$ and G/H has a monomial form on the basis $\{X_1, \cdots, X_n\}$, where $X_i=T_i^m$ $(1\leqq i\leqq n)$. If we regard G as a subgroup of $GL_n(R)$, then the sequence $1\rightarrow D(G/H)\rightarrow G/H\rightarrow\Pi_n(R)\rightarrow 1$ is exact and $\Pi_n(R)$ is contained in G/H. If $\tilde{P}(D(G/H))\neq\{E_n\}$, we continue this procedure. So we may assume that $\tilde{P}(D(G/H))=\{E_n\}$. In this case, by (2.2), $R[X_1, \cdots, X_n]^{G/H}$ is a polynomial ring over R.

§ 3. Unipotent abelian groups

We will consider about invariants of subgroups of the group:

$$A(m, n : q)=\left\{\begin{bmatrix} E_m & 0 \\ M & E_n \end{bmatrix} : \ M \in Mat_{n\times m}(\boldsymbol{F}_q)\right\}.$$

We preserve the following notation in this section.

NOTATION 3.1. *Let $k=\boldsymbol{F}_q$ where $q=p^f$ and p is a prime. Let*

$$\sigma=\begin{bmatrix} E_m & 0 \\ M & E_n \end{bmatrix}, \quad M=[\mu_1\cdots\mu_m]$$

where μ_i $(1\leqq i\leqq m)$ are column vectors. If $\sigma\neq 1$, we put $\varphi(\sigma)=\mu_{i_0}$ where $i_0=min\{i: \mu_i\neq 0\}$. And if $\sigma=1$, put $\varphi(\sigma)=0$. For a subgroup G of the group $A(m, n:q)$, set $d(G)=dim_k\langle\varphi(P(G))\rangle_k$, where $\langle\varphi(P(G))\rangle_k$ is the subspace of the column vector space k^n spanned by the set $\varphi(P(G))$. The group $A(m, n:q)$ acts linearly on the polynomial ring $S=k[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$ in the form that for $\sigma=[\sigma_{ij}]\in A(m, n:q)$

$$({}^t[X_1, \cdots, X_m, Y_1, \cdots, Y_n])^\sigma=[\sigma_{ij}]^t[X_1, \cdots, X_m, Y_1, \cdots, Y_n].$$

LEMMA 3.2. *Let G be a subgroup of $A(m, n:q)$ generated by pseudo-reflections. Then there exists an element $\delta\in GL(n, q)$ such that $Z_i\in S^G$ $(d(G)<i\leqq n)$ where*

$${}^t[Z_1, \cdots, Z_n]=\delta^t[Y_1, \cdots, Y_n].$$

PROOF. Put $d=d(G)$. We can choose elements $\sigma_i\in P(G)$ $(1\leqq i\leqq d)$ such that $\langle\varphi(P(G))\rangle_k=\bigoplus_{i=1}^{d} k\varphi(\sigma_i)$. Hence, for some $\delta\in GL(n, q)$, we have $\varphi(\delta'\sigma_i\delta'^{-1})\in ke_i$ $(1\leqq i\leqq d)$, where $\delta'=diag[1_m, \delta]$ and $\{e_1, \cdots, e_n\}$ is the standard basis of k^n. Since $G=\langle P(G)\rangle$ and $\langle\varphi(P(G))\rangle_k=\bigoplus_{i=1}^{d} k\varphi(\sigma_i)$, this lemma is obvious.

PROPOSITION 3.3. *Let G be a subgroup of $A(m, n:q)$ of order $p^{d(G)}$ generated by pseudo-reflections. Then S^G is a polynomial ring.*

PROOF. Put $d=d(G)$ and choose elements $\sigma_i\in P(G)$ $(1\leqq i\leqq d)$ such that $\langle\varphi(P(G))\rangle_k=\bigoplus_{i=1}^{d} k\varphi(\sigma_i)$. By (3.2) there exists $\Psi'=diag[1_m, \Psi]\in GL(m+n, q)$ such that $\varphi(\Psi'\sigma_i\Psi'^{-1})\in ke_i$ $(1\leqq i\leqq d)$ and $Z_i\in S^G$ $(d<i\leqq n)$, where $\{e_1, \cdots, e_n\}$ is the standard basis of k^n and ${}^t[Z_1, \cdots, Z_n]=\Psi^t[Y_1, \cdots, Y_n]$. Set

$$\Psi'\sigma_i\Psi'^{-1}=\begin{bmatrix} E_m & 0 \\ \tilde{w}_{i1}\cdots\tilde{w}_{im} & E_n \end{bmatrix} \quad (1\leqq i\leqq d).$$

Then we have $\tilde{w}_{ij}=w_{ij}e_i$ $(1\leqq i\leqq d; 1\leqq j\leqq m)$ for some $w_{ij}\in k$. Let

$$W_i=Z_i^p-\left(\sum_{j=1}^{m} w_{ij}X_j\right)^{p-1}Z_i \quad (1\leqq i\leqq d).$$

S^G is integral over $k[X_1, \cdots, X_m, W_1, \cdots, W_d, Z_{d+1}, \cdots, Z_n]$. Since the rings have the common quotient field, we obtain

$$S^G=k[X_1, \cdots, X_m, W_1, \cdots, W_d, Z_{d+1}, \cdots, Z_n].$$

PROPOSITION 3.4. *Let G be a subgroup of $A(1,n:q)$. Then $k[X, Y_1, \cdots, Y_n]^G$ is a polynomial ring and we can construct a system of fundamental invariants of G.*

PROOF. Assume that $|G|>p^{d(G)}$. Choose elements $\sigma_1^{(1)}, \cdots, \sigma_{d(G)}^{(1)} \in G$ such that $\langle\varphi(P(G))\rangle_k=\bigoplus_{i=1}^{d(G)} k\varphi(\sigma_i^{(1)})$. Put $G_1=\langle\sigma_1^{(1)}, \cdots, \sigma_{d(G)}^{(1)}\rangle$, and take a suitable element $\Psi'=diag[1, \Psi]\in GL(n+1, q)$ as we did in the proof of (3.3). Let ${}^t[Z_1, \cdots, Z_n]=\Psi'{}^t[Y_1, \cdots, Y_n]$ and let $W_i=Z_i^p-(w_iX)^{p-1}Z_i$ $(1\leqq i\leqq d(G))$, where the elements $w_i\in k$ $(1\leqq i\leqq d(G))$ are determined by Ψ'. Then we have $k[X, Y_1, \cdots, Y_n]^{G_1}=k[X, W_1, \cdots, W_{d(G)}, Z_{d(G)+1}, \cdots, Z_n]$ and $Z_i\in k[X, Y_1, \cdots, Y_n]^G$ $(d(G)<i\leqq n)$. For $\sigma\in G^{(1)}=G/G_1$, there exist elements $a_\sigma^{(i)}\in k$ $(1\leqq i\leqq d(G))$ which satisfy $W_i^\sigma=W_i+a_\sigma^{(i)}X^p$. Let $\tilde{X}=X^p$ and set

$$\tilde{V}=k\tilde{X}\oplus kW_1\oplus\cdots\oplus kW_{d(G)}\oplus kZ_{d(G)+1}\oplus\cdots\oplus kZ_n.$$

Then $G^{(1)}$ acts linearly and faithfully on the k-space $\tilde{V}$ and we can identify the group $G^{(1)}$ with the image of the canonical homomorphism from $G^{(1)}$ to the group $A(1, d(G):q)$ which is defined on the basis $\{\tilde{X}, W_1, \cdots, W_{d(G)}\}$. If $d(G^{(1)})\neq 0$, then we can construct a subgroup G_2 of $G^{(1)}$ such that $|G_2|=p^{d(G^{(1)})}=p^{d(G_2)}$. By (3.3), $k[X, W_1, \cdots, W_{d(G)}]^{G_2}$ is a polynomial ring. Hence $(k[X, Y_1, \cdots, Y_n]^{G_1})^{G_2}$ is a polynomial ring. Put $G^{(2)}=G^{(1)}/G_2$. If $d(G^{(2)})\neq 0$, then we continue this procedure. Since G is finite, there is an integer $j>0$ such that $d(G^{(j)})=0$. $d(G^{(j)})=0$ implies $G^{(j)}=\{1\}$, and so this proposition is proved.

PROPOSITION 3.5. *Let G be a subgroup of $A(m, 1:q)$. Then $k[X_1, \cdots, X_m, Y]^G$ is a polynomial ring.*

PROOF. First we suppose that G is contained in $A(m, 1:p)$ and $G=\times_{i=1}^{t}\langle\tau_i\rangle$. In this case we may assume that $Y^{\tau_i}=Y+a_iX_i$ $(1\leqq i\leqq t)$ for some elements $a_i\in k$. Put $V_1(T)=T^p-(a_1X_1)^{p-1}T$ and define $V_{i+1}(T)=V_i(T)^p-V_i(a_iX_i)^{p-1}V_i(T)$ $(1\leqq i<t)$ inductively. Then we must have $k[X_1, \cdots, X_m, Y]^G=k[X_1, \cdots, X_m, V_t(Y)]$. Using this result we can prove the general case. The canonical isomorphism $k=\boldsymbol{F}_p1\oplus\boldsymbol{F}_pw_2\oplus\cdots\oplus\boldsymbol{F}_pw_f\ni\sigma\longmapsto(\sigma^{(1)}, \cdots, \sigma^{(f)})\in\boldsymbol{F}_p^f$ as $\boldsymbol{F}_p$-spaces induces a group homomorphism η: $A(m, 1:q)\to A(mf, 1:p)$ defined by

$$\begin{bmatrix} E_m & 0 \\ b_1, \cdots, b_m & 1\end{bmatrix}\longmapsto\begin{bmatrix} E_{mf} & 0 \\ b_1^{(1)}, \cdots, b_1^{(f)}, \cdots, b_m^{(1)}, \cdots, b_m^{(f)} & 1\end{bmatrix}.$$

Let $R=k[X_1^{(1)}, \cdots, X_1^{(f)}, \cdots, X_m^{(1)}, \cdots, X_m^{(f)}, Y]$ be a polynomial ring of $mf+1$ variables with the canonical action of $\eta(G)$. Define a ring homomorphism ρ from R to $S=$

$k[X_1, \cdots, X_m, Y]$ by $\rho(Y)=Y$, $\rho(X_1^{(1)})=X_1$, $\rho(X_1^{(2)})=w_2X_1, \cdots$, $\rho(X_1^{(f)})=w_fX_1, \cdots$, $\rho(X_m^{(1)})=X_m, \cdots$, $\rho(X_m^{(f)})=w_fX_m$. There exists a polynomial $V(Y)\in R$ such that

$$R^{\eta(G)}=k[X_1^{(1)}, \cdots, X_1^{(f)}, \cdots, X_m^{(1)}, \cdots, X_m^{(f)}, V(Y)].$$

Then we obtain $S^G=k[X_1, \cdots, X_m, \rho(V(Y))]$.

THEOREM 3.6. *Let G be a subgroup of $GL_n(k)$ and let $R=k[T_1, \cdots, T_n]$. Then for any minimal prime ideal $\mathfrak{p}$ of R, $R^{I_G(\mathfrak{p})}$ is a polynomial ring and can be determined effectively.*

PROOF. We may assume that $|N|\equiv 0 \ mod\ p$ where $N=I_G(\mathfrak{p})$. There exists a normal p-subgroup H of N such that $([N:H],p)=1$. Since the action of H on R preserves the natural graduation of R, $\mathfrak{p}$ is generated by a homogeneous polynomial of degree 1. Exchanging the basis of $\bigoplus_{i=1}^{n} kT_i$, we can regard H as a subgroup of $A(1, n-1:q)$. By (3.4), R^H is a polynomial ring. N/H is generated by generalized reflections in R^H, therefore $R^N=(R^H)^{N/H}$ is a polynomial ring.

THEOREM 3.7. *Preserve the notation of* (3.6) *and let $I_G^*(\mathfrak{p})=\{{}^t[\sigma_{ij}]:\sigma=[\sigma_{ij}]\in I_G(\mathfrak{p})\}$ for any minimal prime ideal $\mathfrak{p}$ of R. Then $R^{I_G^*(\mathfrak{p})}$ is a polynomial ring.*

PROOF. This theorem is reduced to (3.5).

REMARK 3.8. *Let V be an n-dimensional k-space and let G be an abelian subgroup of $GL(V)$ generated by pseudo-reflections. If $n\leqq 3$, then $k[V]^G$ is a polynomial ring. Suppose that $n=4$ and that $G=Sp(4,p)\cap A(2,2:p)$. Then G is an abelian group generated by transvections, but $k[V]^G$ is not a polynomial ring.*

§4. Symmetric groups

First we will give a remark.

PROPOSITION 4.1. *Let k be a field and let G be a finite group. Let V and W be finite dimensional G-faithful kG-modules. Suppose that there exists a kG-epimorphism $\varphi: V\to W$. If $k[V]^G$ is a polynomial ring, then $k[W]^G$ is a polynomial ring.*

PROOF. Put $g=|G|$. Then $k[V]=\sum_{i=1}^{g} k[V]^G f_i$ for some $f_i\in k[V]$ $(1\leqq i\leqq g)$. It follows that $k[W]=\sum_{i=1}^{g} k[W]^G\tilde{\varphi}(f_i)$, where the homomorphism $\tilde{\varphi}: k[V]\to k[W]$ is the epimorphism induced by φ. Since G acts faithfully on W, $k[W]$ is a free $k[W]^G$-module. Hence $k[W]^G$ is a polynomial ring.

We preserve the following notation from here to (4.4).

NOTATION 4.2. *Suppose that* k *is a finite field of characteristic* $p\neq 2$ *and that* n *is an integer with* $n+2\equiv 0 \bmod p$, $n\geqq 3$. *Let* $\tilde{V}=\bigoplus_{i=0}^{n+1} ke_i$, $V'=\bigoplus_{i=1}^{n+1} k(e_i-e_0)$ *and* $V=V'/k\sum_{i=0}^{n+1} e_i$ *be vector spaces with natural* kS_{n+2}*-module structure, where* S_{n+2} *is the symmetric group of degree* $n+2$. *Let* $\tilde{F}: S_{n+2}\to GL_{n+2}(k)$ (*resp.* $F': S_{n+2}\to GL_{n+1}(k)$) *be the matrix representation of* S_{n+2} *on the basis* $\{e_0, e_1, \cdots, e_{n+1}\}$ (*resp.* $\{e_1-e_0, \cdots, e_{n+1}-e_0\}$) *and put* $\tilde{G}=Im(\tilde{F})$ (*resp.* $G'=Im(F')$). *Let*

$$w=\begin{bmatrix} 1 & & & \\ -1 & 1 & & 0 \\ \vdots & & \ddots & \\ \vdots & 0 & & \ddots \\ -1 & & & & 1 \end{bmatrix}\in GL_{n+2}(k), \quad z=\begin{bmatrix} 1 & 1 & 1\cdots 1 \\ 1 & 2 & 1\cdots 1 \\ 1 & 1 & 2\cdots 1 \\ & \cdots\cdots & \\ 1 & 1 & 1\cdots 2 \end{bmatrix}\in GL_{n+1}(k),$$

$$\tilde{\tilde{G}}=w\tilde{G}w^{-1}, \quad G''=zG'z^{-1}.$$

We denote by G *the subgroup of* $GL_n(k)$

$$\left\{g\in GL_n(k): \begin{bmatrix} 1 & 0 \\ b_g & g \end{bmatrix}\in G''\right\}.$$

Let $\Phi:\tilde{G}\to G'$ (*resp.* $\Psi: G'\to G$) *be the canonical isomorphism* $\tilde{G}\to\tilde{\tilde{G}}\to G'$ (*resp.* $G'\to G''\to G$). *Then the two maps* $P(\tilde{G})\ni\sigma\longmapsto\Phi(\sigma)\in P(G')$, $P(G')\ni\sigma\longmapsto\Psi(\sigma)\in P(G)$ *are bijective.*

LEMMA 4.3. $k[V']^{S_{n+2}}$ *and* $k[V]^{S_{n+2}}$ *are not polynomial rings.*

PROOF. G' (resp. G) acts naturally on the column vector space k^{n+1} (resp. k^n).

(A) Let $G'(a')$ be the stabilizer of G' at a', where $a'={}^t[1, 2, \cdots, p-1, 0, 1, \cdots, p-1, \cdots, 0, 1, \cdots, p-1]\in k^{n+1}$. We identify S_{n+2} with the group of permutation matrices in $GL_{n+2}(k)$. For $\delta\in G'(a')$, there is an element d of $\boldsymbol{F}_p$ such that

$$\Phi^{-1}(\delta)\begin{bmatrix} 0 \\ a' \end{bmatrix}=\begin{bmatrix} 0 \\ a' \end{bmatrix}+\begin{bmatrix} d \\ \vdots \\ d \end{bmatrix}.$$

Since $\Phi^{-1}(\delta)\in P(\tilde{G})$ for $\delta\in P(G'(a'))$, we have $d=0$. Therefore $\Phi^{-1}(P(G'(a')))=\{(i_0, j_0): i_0\equiv j_0 \bmod p, i_0\neq j_0\}\cup\{E_{n+2}\}$. On the other hand

$$\sigma'=\begin{bmatrix} -1 & 1 & & 0 \\ -1 & & 1 & \\ \vdots & & & \ddots \\ \vdots & 0 & & & 1 \\ -1 & & & & \end{bmatrix}\in G'(a'),$$

but σ' is not contained in $\langle P(G'(a'))\rangle$. Since $G'(a')$ is the decomposition group of G' at some maximal ideal of $\bar{k}[V']$, we have shown that $k[V']^{S_{n+2}}$ is not a polynomial ring by (1.4).

(B) For some $a\in k^n$, $za'=\begin{bmatrix}0\\a\end{bmatrix}$. Let $G(a)$ be the stabilizer of G at a. Then $\Psi(G'(a'))=G(a)$. Since $\langle P(G'(a'))\rangle\neq G'(a')$ and $P(G')\ni\tau\longmapsto\Psi(\tau)\in P(G)$ is bijective, we obtain $\langle P(G(a))\rangle\neq G(a)$. Hence $k[V]^{S_{n+2}}$ is not a polynomial ring by (1.4).

REMARK 4.4. *Suppose that V'^* is the dual space of V'. Then $k[V'^*]^{S_{n+2}}$ is a polynomial ring over k by* (4.1).

THEOREM 4.5. *Let k be a finite field of characteristic $p\neq 2$ and let V be a faithful linear representation of least degree of S_n with $n\geqq 7$. Then the following conditions are equivalent*:

(1) *$k[V]^{S_n}$ is a polynomial ring.*

(2) *$(n,p)=1$ and all transpositions of S_n are represented by reflections in $GL(V)$.*

And if V satisfies these conditions, then we have $dim(V)=n-1$.

PROOF. According to [10] and (4.3), it is sufficient to show that (2) implies (1). We can obtain the kS_n-module V as in (2) as follows. Let $\tilde{V}$ be a canonical representation of S_n of degree n. Since $(n,p)=1$, the sequence $0\to\tilde{V}^{S_n}\underset{i}{\to}\tilde{V}\to Coker(i)\to 0$ is a split exact sequence of kS_n-modules and $Coker(i)$ is kS_n-isomorphic to V. Therefore, by (4.1), $k[V]^{S_n}$ is a polynomial ring over k.

§ 5. Classical groups

In this section k is a finite field of characteristic $p\neq 2$.

THEOREM 5.1. *Let G be a subgroup of $GL_2(k)$. Suppose that $T(G)=\phi$ in the case of $p=3$. Then $k[T_1, T_2]^G$ is a polynomial ring if and only if G is generated by pseudo-reflections.*

PROOF. We have only to show the if part. Assume that G is generated by pseudo-reflections. Since $T(G)=\phi$ implies $(|G|,p)=1$, $k[T_1, T_2]^G$ is a polynomial ring in the case of $T(G)=\phi$. Suppose that $T(G)\neq\phi$ and let $H=\langle T(G)\rangle$. Then we have $(|G/H|,p)=1$. If G is reducible, we may assume that H is contained in $A(1,1:q)$. Since $k[T_1, T_2]^H$ is a polynominal ring, $k[T_1, T_2]^G=(k[T_1, T_2]^H)^{G/H}$ is regular by (1.3). Hence, by (2.4), we can suppose that G is irreducible primitive. By Clifford's theorem ([12], § 49), H is irreducible and H is conjugate in $GL_2(k)$ to $SL(2,q)$. It is known that $k[T_1, T_2]^H$ is a polynomial ring. By (1.3), $k[T_1, T_2]^G$ is regular. Thus the proof is completed.

THEOREM 5.2. *For a transvection group* $G \subseteqq GL_n(k)$ $(n \geqq 3)$, *the following conditions are equivalent*:

(1) $k[T_1, \cdots, T_n]^G$ *is a polynomial ring over* k.

(2) G *is conjugate in* $GL_n(k)$ *to* $SL(n, q)$.

PROOF. According to (1.6), it suffices to prove that $k[T_1, \cdots, T_n]^G$ is not a polynomial ring for $G = Sp(n, q)$ or $SU(n, q^2)$. Put $S = k[T_1, \cdots, T_n]$.

(A) First we suppose that $n=4$ and $G = Sp(4, q)$. Let $\{T_1, T_2, T_3, T_4\}$ be the canonical basis on which G can be expressed in the form $\{\sigma \in SL(4, q) : {}^t\sigma \Phi \sigma = \Phi\}$ where

$$\Phi = \begin{bmatrix} 0 & E_2 \\ -E_2 & 0 \end{bmatrix}.$$

Take maximal ideals $\mathfrak{m}_1 = (T_1 - 1, T_2, T_3, T_4)$, $\mathfrak{m}_2 = (T_1, T_2 - 1, T_3, T_4)$, $\mathfrak{m}_3 = (T_1, T_2, T_3 - 1, T_4)$, $\mathfrak{m}_4 = (T_1, T_2, T_3, T_4 - 1)$ of S and put $H = \bigcap_{i=1}^{2} D_G(\mathfrak{m}_i)$, $N = \langle D_H(\mathfrak{m}_3), D_H(\mathfrak{m}_4) \rangle$. Then there exist homogeneous polynomials X_1, X_2 of degree q such that $S^N = k[T_1, T_2, X_1, X_2]$. We regard $S^N = \bigoplus_{i=0}^{\infty} (S^N)_i$ and $S^H = \bigoplus_{i=0}^{\infty} (S^H)_i$ as graded subalgebras of S. Assume that S^H is a polynomial ring. Since $dim_k(S^H)_1 = 2$, there are homogeneous polynomials f_1, f_2, which satisfy $S^H = k[T_1, T_2, f_1, f_2]$. S^N is integral over S^H and so the set $\{T_1, T_2, f_1, f_2\}$ is a system of parameters of S^N at origin. Let $\varphi : S^N \to k[X_1, X_2] \subseteqq S$ be a ring homomorphism defined by $\varphi(T_1) = \varphi(T_2) = 0$ and $\varphi(X_i) = X_i$ $(i=1, 2)$. From $\varphi(f_i) \neq 0$, we obtain $deg(f_i) = deg(\varphi(f_i))$ in S $(i=1, 2)$. Hence $deg(f_i)$ is a power of q. But $|H| = q^3 = \prod_{i=1}^{2} deg(f_i)$ and $\varphi((S^H)_q) = \varphi((S^N)_q)^{H/N}) = 0$, which is a contradiction. Therefore S^G is not a polynomial ring by (1.4). The general case is reduced to the case of $Sp(4, q)$ with aids of (1.2) and (1.4).

(B) We consider the case of $G = SU(n, q^2)$. It is sufficient to prove the assertion for $n=3$. Let $\lambda \longmapsto \bar{\lambda}$ be an involutory automorphism of the field $\boldsymbol{F}_{q^2}$, and let $\varepsilon \in \boldsymbol{F}_{q^2}^*$ be an element such that $Tr(\varepsilon) = 0$. We denote

$$\Gamma(q^2) = \{\sigma \in SL(3, q^2) : {}^t\bar{\sigma} \Psi \sigma = \Psi\}$$

where

$$\Psi = \begin{bmatrix} 0 & \varepsilon & 0 \\ -\varepsilon & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Suppose that H is the stabilizer of $\Gamma(q^2)$ at ${}^t[1, 0, 0]$ under the natural action of $\Gamma(q^2)$

on the column vector space $F_{q^2}^3$ over F_{q^2}. It is easy to show that H is not generated by pseudo-reflections in $GL(3, q^2)$. Since G is conjugate to $\Gamma(q^2)$, S^G is not a polynomial ring by (1.4).

We give the following remark which is a generalization of the preceding result without its proof.

REMARK 5.3. *Let G be an irreducible subgroup of $GL_n(k)$ which contains a transvection and suppose $n \geqq 4$. Then $k[T_1, \cdots, T_n]^G$ is a polynomial ring if and only if G is generated by pseudo-reflections and the normal subgroup $\langle T(G) \rangle$ is conjugate to $SL(n, q)$ in $GL_n(k)$.*

THEOREM 5.4. *Let F be a subfield of k and let $\mathcal{O}$ be the orthogonal group of a non-singular quadratic form Q of dimension n over F. Suppose that G is a subgroup of $\mathcal{O}$ which contains the commutator subgroup Ω of $\mathcal{O}$. If $n \geqq 4$, then $k[T_1, \cdots, T_n]^G$ is not a polynomial ring over k.*

PROOF. Let ν be the index of Q and let V be the n-dimensional F-space with the quadratic form Q. For a subgroup N of $\mathcal{O}$, we denote by $N(x)$ the stabilizer of N at $x \in V$ under the natural action of N on V. Let W be a suitable maximal totally isotropic subspace of V. If $n = 2\nu$, then we have $H = \bigcap_{x \in W} \mathcal{O}(x) \cong F^{\nu(\nu-1)/2}$. In general V can be expressed as an orthogonal direct sum of hyperbolic planes M_i $(1 \leqq i \leqq \nu)$ and a quadratic space L of index 0. Hence, if $\nu \geqq 2$, we obtain $H' = \bigcap_{x \in W} \mathcal{O}'(x) \cong F^{\nu(\nu-1)/2}$ where $\mathcal{O}' = \bigcap_{x \in L} \mathcal{O}(x)$. Suppose that $\nu \geqq 2$. Consequently we can take maximal ideals $\mathfrak{m}_i$ $(1 \leqq i \leqq \nu+2)$ of $\bar{k}[T_1, \cdots, T_n]$ such that

$$F^{\nu(\nu-1)2/} \cong \bigcap_{i=1}^{\nu+2} D_{\mathcal{O}}(\mathfrak{m}_i) = \bigcap_{i=1}^{\nu+2} D_{S\mathcal{O}}(\mathfrak{m}_i)$$

where

$$S\mathcal{O} = SL_n(k) \cap \mathcal{O} .$$

Since $S\mathcal{O}/\Omega \cong F^*/F^{*2} \cong \boldsymbol{Z}/2\boldsymbol{Z}$, $\bigcap_{i=1}^{\nu+2} D_\Omega(\mathfrak{m}_i) \neq \{1\}$ follows. On the other hand we have $P\left(\bigcap_{i=1}^{\nu+2} D_{\mathcal{O}}(\mathfrak{m}_i)\right) = \{1\}$. Hence $\bigcap_{i=1}^{\nu+2} D_G(\mathfrak{m}_i)$ is not generated by pseudo-reflections. Next we assume that $\nu = 1$. Then it follows that $n = 4$ and $\mathcal{O} = O_4^-(F)$. Take an isotropic point and a non-isotropic point of V appropriately. Then we can choose maximal ideals $\mathfrak{n}_1, \mathfrak{n}_2$ of $\bar{k}[T_1, T_2, T_3, T_4]$ such that $\left|\left\langle P\left(\bigcap_{i=1}^{2} D_{O_4^-(F)}(\mathfrak{n}_i)\right)\right\rangle\right| = 2$ and $\bigcap_{i=1}^{2} D_{SO_4^-(F)}(\mathfrak{n}_i) \cong F$ where $SO_4^-(F) = SL_4(k) \cap O_4^-(F)$. Since $|SO_4^-(F)/\Omega| = 2$, $\bigcap_{i=1}^{2} D_G(\mathfrak{n}_i)$ is not generated by pseudo-reflections. In both cases $k[T_1, \cdots, T_n]^G$ is not a polynomial ring by (1.4).

REMARK 5.5. *Let $G \subseteqq GL_n(k)$ be a reflection group and let $n > 3$, $p > 7$. Then*

$k[T_1, \cdots, T_n]^G$ is a polynomial ring over k if and only if G is conjugate in $GL_n(k)$ to one of the groups in the following list:

(i) *The symmetric group S_{n+1} where $n+1 \not\equiv 0 \bmod p$.*

(ii) *The groups in part* (3) *of* (1.7).

This follows from (1.3), (1.7), (4.3), (4.4) and (5.4).

References

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

[2] Bourbaki, N., Groupes et algèbres de Lie, Chapitre 5, Groupes engendrés par des réflexions, Hermann, Paris, 1968.

[3] Chevalley, C., Invariants of finite groups generated by reflections, Amer. J. Math. 77 (1955), 778–782.

[4] Coxeter, H. S. M., The product of generators of a finite group generated by reflections, Duke Math. J. 18 (1951), 765–782.

[5] Dickson, L. E., A fundamental system of invariants of the general modular linear group with a solution of the form problem, Trans. Amer. Math. Soc. 12 (1911), 75–98.

[6] Serezkin, V. N., Groups of reflections over finite fields of characteristic $p>5$, Preprint, Inst. Mat. Akad. Nauk BSSR, Minsk, 1976.

[7] ———, Reflection groups over finite fields of characteristic $p>5$, Dokl. Akad. Nauk SSSR 227 (1976), 574–575.=Soviet Math. Dokl. 17 (1976), 478–480.

[8] Serre, J.-P., Groupes finis d'automorphismes d'anneaux locaux reguliers, Colloq. d'Alg. E.N.S., 1967.

[9] Shephard, G. C. and Todd, J. A., Finite unitary reflection groups, Canad. J. Math. 6 (1954), 274–304.

[10] Wagner, A., The faithful linear representation of least degree of S_n and A_n of odd characteristic, Math. Z. 154 (1977), 103–114.

[11] Zalesskii, A. E. and Serezkin, V. N., Linear groups generated by transvections, Izv. Akad. Nauk SSSR Ser. Mat. 40 (1976), 26–49.=Math. USSR Izvestija 10 (1976), 25–46.

[12] Curtis, C.W. and Reiner, I., Representation theory of finite groups and associative algebras, Interscience, New York, 1962.

Department of Mathematics
Faculty of Technology
Keio University
Hiyoshi, Yokohama-shi 223
Japan