in Progress in Math 60, Birkhäuser, 1985, 231-250.

Generalized invariants of groups generated by reflections.

Victor G. Kac and Dale H. Peterson

Mathematics Department, M.I.T., Cambridge, MA 02139

§ 0. Introduction.

The celebrated Chevalley-Shephard-Todd theorem says that for a finite group G operating linearly on a finite-dimensional complex vector space V the ring of invariant polynomials is a polynomial ring if and only if G is generated by preudoreflections ($g \in G$ is a pseudoreflection if $\dim(g-I)\cdot V = 1$) [2], [10].

Of course, this theorem holds over a field of arbitrary characteristic p as long as p does not divide the order of G. Also it is well-known [9] that the "only if" part of the theorem holds for arbitrary p (a simple geometric proof of this may be found in [4]). It is equally well-known, however, that the "if" part is false if $p \mid |G|$, and lately there have been a number of works on the classification of those finite pseudoreflection groups for which the ring of invariants is a polynomial ring (see [8] and references there). Furthermore, if G is infinite, then the "if" part is false even over $\mathbb{C}$ [13].

Shephard and Todd [10] (and before them Coxeter [3]) were interested mainly in the geometry of reflection groups, while Chevalley's interest in invariants of reflection groups arose from the topology of compact Lie groups. It is a well-known result of Chevalley that the cohomology algebra over $\mathbb{Q}$ of a connected compact Lie group is isomorphic to a Grassmann algebra on generators of degrees $2d_1-1,\dots,2d_\ell-1$, where $d_1,\dots,d_\ell$ are the degrees of the basic invariants of the Weyl group [1].

We came to consider invariants of reflection groups while trying to compute the cohomology of certain infinite-dimensional analogues of compact Lie groups (whose "Weyl group" is an infinite reflection group). Also, we wanted to have an arbitrary field of coefficients, not just $\mathbb{Q}$. We have found that the answer for the cohomology in question can be given in terms of generalized invariants, not just invariants, of the Weyl group (see [5], [6]).

One of the versions of the definition of generalized invariants is as follows. Let G be a group generated by pseudoreflections r_α, $\alpha \in X$, of a finite-dimensional vector space V over an (arbitrary) field $\mathbb{F}$. Let $S = S(V)$ be the symmetric algebra over V and S^+ its augmentation ideal. For a pseudoreflection r_α, pick a non-zero vector α in $(r_\alpha - 1)\cdot V$ and define a linear operator A_α on S by: $A (P) = (P - r_\alpha \cdot P)/\alpha$. Note that

$$(0.1) \quad A_\alpha(PQ) = A_\alpha(P)Q + r_\alpha(P)A_\alpha(Q) \quad \text{for} \quad P,Q \in S .$$

Put

$$(0.2) \quad J = \{P \in S^+ | A_{\alpha_1} \dots A_{\alpha_k}(P) \in S^+ \quad \text{for every} \quad \alpha_1, \dots, \alpha_k \in X\} .$$

This is an ideal of S called the *ideal of generalized invariants*. Elements of J are called generalized invariants, because J contains the ideal (S^{+G}) generated by invariants with a zero constant term, and $J = (S^{+G})$ if $\operatorname{char} \mathbb{F} = 0$ and G is finite.

The main results of the paper concerning generalized invariants of a pseudoreflection group G are as follows.

Theorem A. (a) J *is generated by an* S-*sequence of homogeneous elements of degrees*, *say*, $d_1, d_2, \dots$.

(b) *If* G *is finite*, *then* $J = (S^+)^G$ *if and only if* $|G| = \prod_i d_i$ ..

Note that if p does not divide $|G|$, then, averaging the generators of J over G, we get $J = (S^{+G})$, and since elements of a regular sequence of homogeneous elements are algebraically independent, we recover the "if" part of the Chevalley-Shephard-Todd theorem.

Using the connection with cohomology of compact Lie groups [5], [6], the degrees of basic generalized invariants for Weyl groups of compact Lie groups have been computed in [5] in all characteristics.

An adequate language in dealing with generalized invaraints is the language of twisted derivations. A *twisted derivation* of an algebra S is a vector space endomorphism A for which there exists an automorphism R of S, the *companion* of A, such that

$$(0.3) \quad A(uv) = A(u)v + R(u)A(v) \quad \text{for all} \quad u,v \in S .$$

As we have seen, given a pseudoreflection of a vector space V, one constructs a twisted derivation of the symmetric algebra $S(V)$ (see

(0.1)).

Other examples of algebras with twisted derivations are provided by cohomology rings of flag varieties of compact Lie groups and their infinite-dimensional analogoues and by relative cohomology algebras of Kac-Moody algebras [6]. In fact the present paper was motivated by the work [6], and may be viewed as the "algebraic part" of it.

Twisted derivations of a ring S typically arise as difference operators, as follows. Given an automorphism R of S, take $A = 1-R$ or a multiple of this. (An example from calculus: $A(f(x)) = \frac{f(x+\Delta x)-f(x)}{\Delta x}$.)

An algebra S with a family of twisted derivations $\{A_\alpha\}_{\alpha\in X}$ and companion automorphisms $\{R_\alpha\}_{\alpha\in X}$ is called an *algebra with twisted derivations*. We define the *ideal of generalized invariants* J of a graded algebra with twisted derivations by (0.2) (the A_α and R_α are assumed to be homogeneous). Our main results on algebras with twisted derivations are as follows:

Theorem B. (a) *Let* S *be a graded algebra with twisted derivations*. *Let* S' *be a graded subalgebra of* S *such that* $A_\alpha\cdot S'\subset S'$ *and* $R_\alpha\cdot S'\subset S'$, *and let* J' *be the ideal of generalized invariants of* S' . *Then* $S/J'S$ *is a free* S'/J'-*module*.

(b) *Let* S *be a graded algebra with twisted derivations and let* J *be the ideal of generalized invariants of* S . *Then* J/J^2 *is a free* S/J-*module*.

Note that Theorem A(a) follows from Theorem B(b) by making use of a result of Vasconcelos [19].

Such freeness results, along with a strong rigidity properties (cf. Proposition 1.1), seem to us to be the most fundamental characteristics of rings with twisted derivations.

Most of this work was done at the University Paris 6 and MSRI during 1983-84 academic year and was partially supported by the NSF grant MCS-8203739.

§1. Rings with twisted derivations.

Throughout the paper by a ring we mean an associative ring with unity and by a module over a ring a unital left module.

A twisted derivation of a ring S is a map $A : S \to S$ with the following two properties:

(A1) $A(s+t) = A(s) + A(t)$ for all $s,t \in S$;

(A2) $A(st) = A(s)t + R(s)A(t)$ for all $s,t \in S$,

where R is an automorphism of the ring S , called the companion automorphism of A .

A ring with twisted derivations (abbreviated RTD) is a quadruple $(S,X,\{A_i\}_{i\in X},\{R_i\}_{i\in X})$, where S is a ring, X is an index set, $\{A_i\}_{i\in X}$ is a family of twisted derivations of S and $\{R_i\}_{i\in X}$ is the family of companion automorphisms, indexed by X . By abuse of terminology, we will sometimes call S itself an RTD. The subgroup of Aut S generated by all companion automorphisms is called the Weyl group of S . A morphism of RTD's $(S,X,\{A_i\}_{i\in X},\{R_i\}_{i\in X}) \to (S',X',\{A_i'\}_{i\in X'},\{R_i'\}_{i\in X'})$ is a ring homomorphism $\phi : S \to S'$ and a bijection $\mu : X \to X'$, such that $\phi\circ A_i = A'_{\mu(i)}\circ\phi$ and $\phi\circ R_i = R'_{\mu(i)}\circ\phi$ for all $i \in X$.

Let $(S,X,\{A_i\},\{R_i\})$ be an RTD and let $W \subset \text{Aut } S$ be its Weyl group. Let I be a W-invariant subset of S . The largest subset of S contained in I which is W-invariant and, in addition, A_i-invariant for all $i \in X$, is called the nucleus of I and denoted by $\text{nucl}(I)$. The set I is called reduced if $\text{nucl}(I) = 0$. Note that

$$\text{nucl } I = \{s \in I \mid \ldots w_2 A_{i_2} w_1 A_{i_1} w_0(s) \in I \text{ for every } w_0,w_1,\ldots \in W \text{ and } i_1,i_2,\ldots \in X\} .$$

Note also that the nucleus of a right (resp. left) ideal is a right (resp. left) ideal.

Note that for a homomorphism ϕ of RTD's we have

(1.1) $\phi^{-1}(\mathrm{nucl}\ I) = \mathrm{nucl}(\phi^{-1}(I))$.

It follows that if I is reduced, then

(1.2) $\mathrm{Ker}\ \phi = \mathrm{nucl}(\phi^{-1}(I))$.

Proposition 1.1 (rigidity of multiplication). Let I be a reduced W-invariant two-sided ideal of an RTD S . Then the multiplicative structure of S is determined uniquely by the additive structure of S , the action of W on S and the multiplicative structure of S/I .

Proof. Suppose that S carries two multiplicative structures st and $s*t$, with the same additive structure, the same action of W and the same multiplicative structure of S/I. Then

$$st - s*t \in I \text{ , and}$$

$$A_i(st-s*t) = (A_i(s)t-A_i(s)*t)+(R_i(s)A_i(t)-R_i(s)*A_i(t)) \in I \text{ .}$$

Similarly, for any word A in the A_i and R_i , $A(st-s*t) \in I$, hence $st-s*t \in \mathrm{nucl}\ I = 0$. □

A module over an RTD $(S,X,\{A_i\},\{R_i\})$ is an abelian group M with the structure of a unital S-module and an action of the A_i by endomorphisms of M and the R_i by automorphisms of M such that the following properties hold:

(M1) $R_i(s\cdot m) = R_i(s)R_i(m)$ for all $i \in X$, $s \in S$, $m \in M$;

(M2) $A_i(s\cdot m) = A_i(s)\cdot m + R_i(s)\cdot A_i(m)$ for all $i \in X$, $s \in S$, $m \in M$.

Given a module M over a ring S and a subset I of S , one says that the elements $m_1,\dots,m_k$ of M are independent modulo I if from $\sum_i s_i m_i \in IM$ for some $s_1,\dots,s_k \in S$, it follows that $s_i \in I$, $i = 1,\dots,k$.

Now we can state the crucial lemma.

Lemma 1.2. Let M be a module over an RTD $(S,X,\{A_i\},\{R_i\})$. Let I be a W-invariant right ideal of S . If $m_1,\dots,m_k$ are elements of M which are independent modulo I , then they are independent modulo nucl (I) .

Proof. Suppose that

(1.3) $\sum_j s_j\cdot m_j \in (\mathrm{nucl}(I))M$.

Then, by the hypothesis, $s_j \in I$ for all j . We have to show that

(1.4) $w_0A_{i_1}w_1\ldots A_{i_n}w_n(s_j) \in I$ for all $w_0,\ldots,w_n \in W$
and all $i_1,\ldots,i_n \in X$.

We prove (1.4) by induction on n , which we call the height of the element $w_0A_{i_1}\ldots A_{i_n}w_n$. Applying this element to both sides of (1.3), we have (by (M2):

$\sum_j (w_0A_{i_1}w_1\ldots A_{i_n}w_n)(w_0\ldots w_n(m_j)) + \sum_i B_i(s_i)\cdot m_i' \in (\text{nucl } I)M \subset IM$,

where the height of B_i is less than n and $m_i' \in M$. Applying the inductive assumption, we get:

$\sum_j (w_0A_{i_1}w_1\ldots A_{i_n}w_n(s_j))\cdot(w_0\ldots w_n(m_j)) \in IM$,

hence (by (M1)), applying $(w_0\ldots w_n)^{-1}$, we get:

$\sum_j ((w_0\ldots w_n)^{-1}(w_0A_{i_1}\ldots A_{i_n}w_n)s_j)\cdot m_j \in IM$.

Therefore, by the independence mod I of the m_j , (1.4) holds. □

§2. Local and graded rings with twisted derivations.

Throughout this section S will be a commutative ring of one of the following two types:

(L) Local ring, i.e. S has a unique maximal ideal S^+.

(G) Graded ring, i.e. $S = \bigoplus_{j\geq 0} S_j$ and $S_iS_j \subset S_{i+j}$; we let $S^+ = \bigoplus_{j>0} S_j$ be the augmentation ideal.

In the local case (L) all S-modules will be assumed to be finitely generated. In the graded case (G), every S-module M will be assumed to be graded, i.e. $M = \bigoplus_{j\geq 0} M_j$ (direct sum of abelain groups) and $S_iM_j \subset M_{i+j}$. A homomorphism of graded rings or modules will be assumed to preserve the gradation.

We will need the following well-known surjectivity result (see e.g. [7] for local case; the graded case is obvious).

Lemma 2.1 (Nakayama lemma). *Let S be a local or graded ring, and let M and N be S-modules. Let $\phi : M \to N$ be a homomorphism such that the induced homomorphism $M/S^+M \to N/S^+N$ is surjective. Then ϕ is surjective.* □

A sequence $a_1,\dots,a_n$ of elements of a ring S is called an S-*sequence* if $S \neq a_1S+\dots+a_nS$ and if the image of a_k in $S/(a_1S+\dots+a_{k-1}S)$ is not a zero divisor, for $k = 1,\dots,n$. If S is graded, the a_i are assumed to be homogeneous.

By a *minimal generating set* for an ideal J of a ring S we mean a set which generates J but such that no proper subset generates J ; in the graded case the generators are assumed to be homogeneous. Note that an S-sequence $a_1,\dots,a_n$ is a minimal generating set of the ideal $a_1S+\dots+a_nS$.

The following fact should be well known.

Lemma 2.2. Let S *be either a Noetherian local ring or a Noetherian graded ring with* S_0 *a field, and let* J *be an ideal of* S *generated by an S-sequence. Then any minimal generating sequence of* J *is an S-sequence.*

Proof. By the Nakayama lemma, a sequence $X = (x_1,\dots,x_p)$ generates J if and only if $X \bmod S^+J$ spans the vector space J/S^+J over the field S/S^+. This fact reduces the case of a graded S to local case by considering the formal completion of S. Let now S be a local ring. The above fact also shows that if $X = (x_1,\dots,x_p)$ and $Y = (y_1,\dots,y_q)$ are minimal generating sequences of J, then $p = q$ and there exists $A \in GL_p(S)$ such that $Y = XA$. But any permutation of an S-sequence is an S-sequence ([7, Theorem 27]). Moreover, if $A \in GL_p(S)$ is lower triangular, then X is a S-sequence if and only if XA is an S-sequence. Since $GL_p(S)$ is generated by permutation matrices and lower triangular matrices, the lemma follows. □

A (local or graded) ring S is called *regular* if it satisfies the following properties

(i) S is Noetherian;

(ii) S^+ is generated by an S-sequence;

(iii) if S is graded, then S_0 is a field.

Lemma 2.3. Let S *be a regular (local or graded) ring, and let* J *be an ideal of* S *such that* J/J^2 *is a free module over* S/J. *Then any minimal generating sequence of* J *is an S-sequence.*

Proof. Since every (finitely generated) module over a regular local ring is of finite projective dimension, in view of Lemma 2.2., the lemma for local S is a special case of a theorem of Vasconcelos [12].

Let now S be a graded ring and let $\hat{S} = \prod_{j\geq 0} S_j$ be the formal completion of S with the unique maximal ideal $\hat{S}^+ = \prod_{j>0} S_j$.

Let $Y = (Y_1,\dots,Y_p)$ be a sequence of homogeneous elements of J such that $Y \bmod J^2$ is a free basis of the module J/J^2 over S/J. We have to show that Y is an S-sequence which generates J. By the Nakayama lemma, Y generates the ideal $\hat{J} := \hat{S}J$ of $\hat{S}$. Clearly, $Y \bmod \hat{J}^2$ is a free basis of the module $\hat{J}/\hat{J}^2$ over $\hat{S}/\hat{J}$ and, hence, is a minimal generating sequence for $\hat{J}$. Since $\hat{S}$ is local, by what has already been shown and Lemma 2.2, Y is an $\hat{S}$-sequence which generates $\hat{J}$, hence it is an S-sequence which generates J . □

We now turn again to rings with twisted derivations. An RTD $(S,X,\{A_i\},\{R_i\})$ is called local (resp. graded) if the ring S is local (resp. graded), the Weyl group preserves S^+ , and the A_i and R_i are homogeneous in the graded case. We call $\mathrm{nucl}(S^+)$ the *ideal of generalized invariants* of the local or graded RTD S ; we call S *reduced* if $\mathrm{nucl}(S^+) = 0$.

Theorem 2.1. *Let* M *be a module over a local or graded RTD* S , *and let* J *be the ideal of generalized invariants*. *Assume that* S_0 *is a field if* S *is graded*. *Then* M/JM *is a free* S/J-*module*.

Proof. Let $m_1,m_2,\ldots \in M$ be such that the m_i mod S^+M form a free basis of the module M/S^+M over S/S^+ . Let F be a free S-module on generators $\bar{m}_1,\bar{m}_2,\ldots,$ and let $\phi : F \to M$ be a module homomorphism defined by $\phi(\bar{m}_i) = m_i$. By Nakajama's lemma, ϕ is surjective, hence the induced homomorphism $\phi_J : F/JF \to M/JM$ is surjective. But the induced homomorphism $F/S^+F \to M/S^+M$ is obviously injective. By Lemma 1.2, it follows that ϕ_J is injective. Thus, ϕ_J is an isomorphism. □

By a graded algebra with twisted derivations (ATD) we mean a graded RTD $(S,X,\{A_i\},\{R_i\})$ such that S_0 is a field and all the A_i and R_i are linear over S_0 . The following theorem summarizes the most important properties of graded ATD's.

Theorem 2.2. (a) *Let* $\phi : S \to S'$ *be a homomorphism of graded RTD's such that* $\phi : S_0 \to S_0'$ *is injective, and let* J *be the ideal of generalized invariants of* S. *Then* $\mathrm{Ker}\,\phi = J$ *if* S' *is reduced*.

(b) *Let* S *be a graded ATD and let* S' *be a subalgebra of* S *which is invariant under all the* A_i *and* R_i . *Let* J' *be the ideal of generalized invariants of* S' . *Then* $S/J'S$ *is a free module over* S'/J' . *In particular*, S *is a free module over* S' *if* S' *is reduced*.

(c) *Let* S *be a graded ATD and let* J *be the ideal of generalized invariants*. *Then* J/J^2 *is a free* S/J-*module*.

(d) *Let* S *be a graded ATD which is a polynomial algebra (in finite number of indeterminates)*. *Then any minimal* *generating sequence of the ideal of generalized invariants of* S *is an* S*-sequence*.

Proof. (a) follows from (1.2). (b) follows from Theorem 2.1 applied to the S'-module S. (c) follows from Theorem 2.1 applied to the S-module J. (d) follows from (c) and Lemma 2.3. □

We shall need one more statement about graded ATD.

Lemma 2.4. *Let* $(S,X,\{A_i\},\{R_i\})$ *be a graded ATD*. *Denote by* $\mathfrak{A}$ *the algebra of operators on* S *generated by the* A_i, R_i, R_i^{-1}. *Let* J *be the ideal of generalized invariants of* S *and let* $Q_1,\ldots,Q_N$ *be a sequence of homogeneous elements of* S *of non-increasing degrees, which are linearly independent* mod J *over* S_0. *Then*

(a) *There exists* $A \in \mathfrak{A}$ *such that* $A(Q_1) = 1$ *and* $A(Q_j) = 0$ *for* $j > 1$.

(b) *The* Q_i *are linearly independent over* $S^{\mathfrak{A}} := \{s \in S | A_i(s) = 0$ *and* $R_i(s) = s$ *for all* $i \in X\}$.

Proof. (a) is obvious. To prove (b), note that for $A \in \mathfrak{A}$, $s \in S^{\mathfrak{A}}$ and $t \in S$, we have $A(st) = sA(t)$. Suppose $s_1,\ldots,s_N \in S^{\mathfrak{A}}$ and $\Sigma s_iQ_i = 0$. By (a), choose $A \in \mathfrak{A}$ such that $A(Q_1) = 1$ and $A(Q_j) = 0$ for $j > 1$. Then $0 = A(\Sigma s_iQ_i) = \Sigma s_iA(Q_i) = s_1$. By induction on N, this proves (b). □

§3. Generalized invariants of groups generated by pseudoreflections.

Let M be a module over a commutative ring $\mathbb{F}$. Given a non-zero $\alpha \in M$ and a non-zero $\phi \in \mathrm{Hom}_{\mathbb{F}}(M,\mathbb{F})$ such that $1+\phi(\alpha)$ is an invertible element of $\mathbb{F}$, we define a pseudoreflection r_α of M by

$$r_\alpha(m) = m + \phi(m)\alpha \quad \text{for} \quad m \in M .$$

One easily checks that r_α is an automorphism of M. Furthermore, r_α extends uniquely to an automorphism R_α of the symmetric algebra $S(M) = \bigoplus_{k\geq 0} S^k(M)$ fixing $\mathbb{F}$.

Let $\{r_\alpha\}_{\alpha\in X}$ be a collection of pseudoreflections of the module M, and let G be the subgroup of $\mathrm{Aut}\, M$ generated by it. Then the pair $(G,\{r_\alpha\}_{\alpha\in X})$ is called a pseudoreflection group.

Let $\mathbb{F}$ be an integral domain and let M be a free module over $\mathbb{F}$. Then one easily checks by induction on k, that for $P \in S^k(M)$, there exists a unique $P_1 \in S^{k-1}(M)$ such that $P - R_\alpha(P) = P_1\alpha$. Putting $A_\alpha(P) = P_1$ gives a twisted derivation A_α of $S(M)$ with the companion automorphism R_α. (Note that r_α determines A_α up to a non-zero constant factor.)

Thus a pseudoreflection group $(G,\{r_\alpha\}_{\alpha\in X})$ on a free module M over an integral domain gives rise to an RTD $(S(M),X,\{A_\alpha\}_{\alpha\in X},\{R_\alpha\}_{\alpha\in X})$, and hence to the ideal of generalized invariants J of $S(M)$. Note that J contains the ideal J_0 generated by homogeneous G-invariant elements of $S(M)$ of positive degree.

From now on we will assume that M is a finite-dimensional vector space over the field $\mathbb{F}$.

Theorem 2.2(d) implies immediately

Theorem 3.1. *Let $(G,\{r_\alpha\})$ be a pseudoreflection group on a finite-dimensional vector space M. Then any minimal generating sequence of the ideal of generalized invariants J of $S(M)$ is an $S(M)$-sequence.* □

Remark 3.1. Let G be a pseudoreflection group such that each generating pseudoreflection has finite order which is prime to char $\mathbb{F}$. Then the ideal J of generalized invariants can be constructed as follows. Define by induction an ascending sequence of ideals J_k $(k = -1,0,1,\dots)$ of $S(M)$ by putting $J_{-1} = \{0\}$, J_k = ideal generated by $\{a \in S(M)^+ / g \cdot a - a \in J_{k-1}$ for all $g \in G\}$ for $k \geq 0$; then $J = \bigcup_{k \geq -1} J_k$. Indeed, by induction on s one shows that if $\deg x = s$ and $A_{i_1} \dots A_{i_s}(x) = 0$ for every sequence $i_1,\dots,i_s \in X$, then $x \in J_{s-1}$. To prove that $\bigcup_k J_k \subset J$, one has to show that a homogeneous element u of positive degree of $S(M)/J$, fixed by G, is zero. Let $r_i^N = 1$ and $N \neq 0$ in $\mathbb{F}$. We have: $NA_i(u) = NA_i(u) - A_i((R_i + \dots + R_i^N)u) = A_i(\sum_{k=1}^{N} (u - R_i^k u)) \in A_i(J) \subset J$. It follows that $A_i(u) \in J$ and hence $u \in J$.

In particular, we see that in this case J is independent of the choice of the generating set of G. This is false in general (see Example 3.1(e)).

A natural problem is to characterize all linear groups G (not necessarily pseudoreflection groups) such that the ideal $\bigcup_k J_k$ is is generated by an $S(M)$-sequence. (If $|G| < \infty$ and char $\mathbb{F}$ does not divide $|G|$, the answer is provided by the Chevalley-Shephard-Todd theorem.)

Note that the identity $A_i(\alpha_i Q) = Q + R_i(Q)$ shows that over a field of characteristic 2, if G is a finite group generated by reflections (i.e. involutive pseudoreflections), then the top graded piece of $S(M)/J$ is fixed under G, and therefore $\bigcup_k J_k \neq J$. □

We shall need the following simple facts about graded algebras.

Lemma 3.1. Let S be a graded commutative ring with $\mathbb{F} := S_0$ a field. Let I (resp. Y) be the ideal (resp. subalgebra) of S generated by a sequence of homogeneous elements $y_1,\dots,y_r$. Let Z be a homogeneous $\mathbb{F}$-subspace of S such that $S = Z \oplus I$ (direct sum of vector spaces over $\mathbb{F}$). Then

(a) $y_1,\dots,y_r$ is a minimal generating sequence of I if and only if *the* y_i mod (S^+I) *form a basis over* $\mathbb{F}$ *of* I mod (S^+I) .

(b) $S = YZ$.

(c) *If* $y_1,\ldots,y_r$ *is an* S-*sequence, then* Y *is a polymonial algebra over* $\mathbb{F}$ *on the* y_i *and the map* $\phi : Y \otimes_{\mathbb{F}} Z \to S$ *defined by* $\phi(y \otimes z) = yz$ *is an isomorphism of* Y-*modules*.

Proof. (a) follows from the Nakayama lemma. (b) is clear by using the grading. (c) is proved by induction on r , by considering $S/(y_1)$. □

Now let $(G,\{r_\alpha\})$, etc., be as in Theorem 3.1, and let $P_1,P_2,\ldots$ be a minimal generating sequence of the ideal J of generalized invariants. By Lemma 3.1(a), the $d_i := \deg P_i$, ordered by $d_1 \leq d_2 \leq \ldots$, are independent of the choice of $P_1,P_2,\ldots$. By Theorem 3.1 and Lemma 3.1(c), we find that the Poicaré series of the graded algebra $S(M)/J$ is

$$(3.1)\quad (1-t)^{-\dim M}\prod_i (1-t^{d_i}) .$$

We will need the following two well-known properties of the action of a finite linear group G on a finite-dimensional vector space M :

$$(3.2)\quad \mathrm{Fract}\ S(M) = S(M)\ \mathrm{Fract}\ S(M)^G .$$

$$(3.3)\quad \dim_{\mathrm{Fract}(S(M)^G)} \mathrm{Fract}\ S(M) = |G| .$$

(Here and below, Fract stands for the field of fractions.)

By Lemma 2.4(b) and (3.3), we have:

$$(3.4)\quad \dim_{\mathbb{F}} S(M)/J \leq |G| .$$

That is, by (3.1):

$$(3.5)\quad \prod d_i \leq |G| .$$

Now we will prove the following theorem.

Theorem 3.2. *Let* G *be a finite pseudoreflection group on a finite-dimensional vector space* M *and let* $d_1,d_2,\ldots$ *be the degrees of a minimal generating sequence of the ideal* J *of generalized invariants of* $S(M)$. *Then* $|G| = \prod_i d_i$ *if and only if* $J = J_0$, *where* J_0 *is the ideal of* $S(M)$ *generated by the homogeneous* G-*invariants of positive degree*.

Proof. Put $D = \Pi d_i$. By (3.1) and (3.4), choose a sequence $Q_1, \ldots, Q_D$ of homogeneous elements of $S(M)$ forming an $\mathbb{F}$-basis of $S(M)$ mod J, with $\deg Q_1 \geq \deg Q_2 \geq \ldots$.

Suppose $J = J_0$. By Lemma 3.1(b), the $S(M)^G$-module $S(M)$ is generated by the Q_j. Hence, by (3.2), the (Fract $S(M)^G$)-module Fract $S(M)$ is generated by the Q_j. Hence, by (3.3) $D \geq |G|$, so that $D = |G|$ by (3.5).

Now suppose $D = |G|$. Then, by (3.3) and Lemma 2.4(b), the Q_j form a basis of Fract $S(M)$ over Fract$(S(M)^G)$. We will prove that the Q_j form a basis of $S(M)$ over $S(M)^G$. This granted, the Q_j span $S(M)/J_0$ over $\mathbb{F}$. Since $J_0 \subset J$, this forces $J_0 = J$, proving the theorem.

It remains to show that the Q_j generate the $S(M)^G$-module $S(M)$. Let $Q \in S(M)$ be given. Since the Q_j generate the module Fract $S(M)$ over Fract$(S(M)^G)$, there exist $r, r_1, \ldots, r_D \in S(M)^G$ satisfying

$$(3.6) \quad rQ = \Sigma\, r_i Q_i \, .$$

We must show that r divides all the r_i.

If not, let r divide $r_1, \ldots, r_{k-1}$, but not divide r_k. We may assume that $r_1 = \ldots = r_{k-1} = 0$. By Lemma 2.4a, choose $A \in$ such that $A(Q_k) = 1$ but $A(Q_j) = 0$ for $j > k$. Applying A to both sides of (3.6), we get $rA(Q) = r_k$, so that r divides r_k, a contradiction. This proves the theorem. □

Remark 3.2. Let G be a finite pseudoreflection group operating on a finite-dimensional vector space M over a field $\mathbb{F}$ of characteristic p. If p' is a prime differnt from p, and H is a p'-Sylow subgroup of G, then (by averaging) one can choose a minimal generating sequence $P_1, P_2, \ldots$ (of degrees $d_1, d_2, \ldots$) of the ideal of generalized invariants J to be in $S(M)^H$. Let $R = \mathbb{F}[P_1, P_2, \ldots]$. Then we have: Fract $R \subset$ Fract $S(M)^H \subset$ Fract $S(M)$. It follows from (3.3) and Lemma 3.1(c) that $|H|$ divides $\prod_i d_i$. Thus, we have

$$(3.7) \quad \frac{|G|}{p^s} \text{ divides } \prod_i d_i \text{ , where } p^s \| \, |G| \, .$$

We conjecture that always $|G| = p^t \prod_i d_i$, where $t \geq 0$.

Example 3.1. Let V be a vector space of finite dimension n over a field $\mathbb{F}$, and let p be the characteristic of $\mathbb{F}$. Let R_1 and R_2 be distinct pseudoreflections on V such that R_1R_2 is of finite order m and $R_1^2 = R_2^2 = I$. Let G be the subgroup of $GL(V)$ generated by R_1 and R_2 . Let $V^G = \{v \in V | g(v) = v$ for all $g \in G\}$. Let $\alpha_1, \alpha_2 \in V$ satisfy $(I-R_i)V = \mathbb{F}\alpha_i$, and define operators A_1, A_2 on $S(V)$ by $u-R_i(u) = \alpha_i A_i(u)$. Let J be the ideal of generalized invariants of $S(V)$ associated to G and A_1, A_2 . Let $J_0, J_1, J_2, \ldots$ be the ideals of $S(V)$ associated to G defined in Remark 3.1 and let $J = \bigcup_k J_k$. Let $\mathfrak{A}_0$ be the $\mathbb{F}$-algebra of operators on $S(V)$ generated by A_1 and A_2 . A detailed calculation then verifies:

(a) If m is odd, assume that $\alpha_2 = (R_1R_2)^{\frac{1}{2}(m-1)} \alpha_1$. Then $\mathfrak{A}_0$ is the unital $\mathbb{F}$-algebra on generators A_1 and A_2 with defining relations:

$$A_1^2 = A_2^2 = 0 \text{ , and}$$

(3.8) $A_1A_2A_1\ldots = A_2A_1A_2\ldots$ (m factors on each side).

(b) The following conditions are equivalent: $\dim(V/V^G) = 2$; $J = J_0$; $\mathfrak{A}_0$ acts faithfully on S/J .

(c) $J_2 = J_3 = J_4 = \ldots$.

We also have:

(d) J_0 is generated by an $S(V)$-sequence of homogeneous elements. If $\dim(V/V^G) = 2$, then the degrees of $J/VJ = J_0/VJ_0$ are: $d_i = 1$, $1 \leq i \leq n-2$; $d_{n-1} = 2$; $d_n = m$. If $\dim(V/V^G) = 1$, then the degrees of J/VJ are: $d_i = 1$, $1 \leq i \leq n-1$; $d_n = 2$; and the degrees of J_0/VJ_0 are: $e_i = 1$, $1 \leq i \leq n-1$; $e_n = 2m$.

(e) Let $\tilde{J}$ be the ideal of generalized invariants of $S(V)$ associated to the set of <u>all</u> pseudoreflections in G . Then $\tilde{J} = J_0$ if G is generated by semisimple pseudoreflections. (In particular, $J \neq \tilde{J}$ if $p \neq 2$ and $\dim(V/V^G) = 1$.)

(f) Consider the following <u>Condition A</u>: If U is a subspace of V , then $G_U := \{g \in G | g = I$ on $U\}$ is generated by at most $\dim(V/U)$ pseudoreflections. Then the following implications hold: $|G| \neq 0$ in $\mathbb{F}$ => Condition A => $J = J_0$.

(g) If $p = 2$ and $A_1(\alpha_2)A_2(\alpha_1) \neq 0$, then $(J_0, S^m(V)) = J_1 =$

$J_2 = \dots$; in particular, none of $J_1 = J_2 = \dots = J$ is generated by an $S(V)$-sequence of homogeneous elements.

Questions. Do (e) and (f) hold for arbitrary pseudoreflection groups? If G is generated by k pseudoreflections, is it true that $J_k = J_{k+1} = J_{k+2} = \dots$? □

In view of their importance, we indicate a simple proof of the "braid relation" (3.8) in (a).

Proposition 3.1. Let S *be a ring with unity. Let* A_1, A_2 *be twisted derivations of* S *with companion automorphisms* R_1, R_2 . *Let* W *be the subgroup of* $\mathrm{Aut}(S)$ *generated by* R_1 *and* R_2 . *Let* m *be a positive integer, let* $k \in \{1,2\}$ *satisfying* $k-m \in 2\mathbb{Z}$, *and put* $T = R_1R_2R_1 \dots$ (m *factors*). *Assume:*

(i) *For* $i = 1,2$, $A_i^2 = 0$, *and there exists* $\lambda_i \in \mathrm{center}(S)$ *satisfying* $A_i(\lambda_i) = 1$.

(ii) A_1A_2 *and* A_2A_1 *kill* $W(\lambda_k)$, *and* $A_2T(\lambda_k) = -1$.

(iii) $A_2A_1A_2 \dots = 0$ (m+1 *factors*).

Then:

(a) *For* $i = 1,2$, $A_iR_i = A_i = R_iA_i$, $R_i^2 = 1$, $\mathrm{Im}\, A_i = \mathrm{Ker}\, A_i$; *for all* $z \in S$, *there exist unique* $x,y \in \mathrm{Im}\, A_i$ *such that* $z = \lambda_i x + y$.

(b) $A_1A_2A_1 \dots = A_2A_1A_2 \dots$ (m *factors on each side*).

Proof. Put $\alpha_i = \lambda_i - R_i(\lambda_i)$, so that $\alpha_i \in \mathrm{center}(S)$. Let $z \in S$. Since A_i is a twisted derivation and $A_i(\lambda_i) = 1$, we have

(1) $A_i(z\lambda_i) = A_i(z)\lambda_i + R_i(z)$,

(2) $A_i(\lambda_i z) = z + R_i(\lambda_i)A_i(z)$.

Equating these we have

(3) $z - R_i(z) = \alpha_i A_i(z)$.

Since $A_i^2 = 0$, (3) gives $A_i = R_iA_i$.
Since $A_i^2 = 0$, (2) gives $\mathrm{Im}\, A_i = \mathrm{Ker}\, A_i$.
By (1), $A_iR_i(z) = A_i(A_i(z\lambda_i) - \lambda_i A_i(z)) = -A_i(\lambda_i)A_i(z) = -A_i(z)$ since A_i is a twisted derivation, $A_i^2 = 0$ and $A_i(\lambda_i) = 1$. Hence, by (3), $R_i^2(z) = R_i(z) - \alpha_i A_i R_i(z) = R_i(z) + \alpha_i A_i(z) = R_i(z) + (z - R_i(z)) = z$. By (1) and $A_i^2 = 0$, for every $v \in S$ there exist $t,u \in \mathrm{Ker}\, A_i$ such that $v = \lambda_i t + u$; moreover, if $v = 0$, then $0 = A_i(v) = A_i(\lambda_i t + u) = A_i(\lambda_i)t = t$ forces $t = u = 0$. This proves (a).

We now prove (b). We first show that for $\lambda \in W(\lambda_k)$ and $z \in S$,

(3.9) $A_2A_1(\lambda A_2(z)) = A_2(R_1(\lambda)A_1A_2(z))$ and $A_1A_2(\lambda A_1(z)) = A_1(R_2(\lambda)\ A_2A_1(z))$.

Indeed, since A_1 is a twisted derivation, $A_1(\lambda A_2(z)) = A_1(\lambda)A_2(z) + R_1(\lambda)A_1A_2(z)$, and since A_2 is a twisted derivation, $A_2(A_1(\lambda)A_2(z)) = A_2A_1(\lambda)A_2(z) + R_2A_1(\lambda)A_2^2(z)$, which is 0 by (i) and (ii). This verifies the first equality; the second is verified similarly. Now suppose $m = 2r$ and $z \in S$. Applying (2) and (iii), we have $(A_2A_1)^r(z) = (A_2A_1)^r(A_2(\lambda_2 z) - R_2(\lambda_2)A_2(z)) = -(A_2A_1)^r(R_2(\lambda_2)A_2(z))$. But by applying (3.9) successively, we obtain $(A_2A_1)^r(R_2(\lambda_2)A_2(z)) = (A_2A_1)^{r-1}A_2(R_1R_2(\lambda_2)A_1A_2(z)) = \dots = A_2((R_1R_2)^r(\lambda_2)(A_1A_2)^r(z))$. Using (iii) and the fact that A_2 is a twisted derivation, we see that this equals $A_2(R_1R_2)^r(\lambda_2)(A_1A_2)^r(z)$ which equals $-(A_1A_2)^r(z)$ by (ii). Combining these verifies (b) if $m = 2r$. Similarly, if $m = 2r+1$, then $(A_2A_1)^rA_2(z) = -(A_2A_1)^rA_2(R_1(\lambda_1)A_1(z)) = \dots = -A_2((R_1R_2)^rR_1(\lambda_1)(A_1A_2)^rA_1(z)) = -A_2(R_1R_2)^rR_1(\lambda_1)(A_1A_2)^rA_1(z) = (A_1A_2)^rA_1(z)$. This proves (b). □

To prove the braid relation (3.8), it therefore suffices to verify the hypotheses (i), (ii) and (iii) of Proposition 3.1.(i) is clear. The first part of (ii) is trivial and the second not difficult. If $\dim(V/V^G) = 2$, then the assertion (d) about J_0 of the Example 3.1 implies that $S(V) = S(V)^G \sum_{k=0}^{m} S^k(V)$, which implies the hypotheis (iii). If $\dim(V/V^G) = 1$, then the assertion (d) about J_0 of the Example 3.1 implies that $S(V) = S(V)^G \sum_{k=0}^{2m-1} S^k(V)$. If $m = 2$, then this forces $A_2A_1A_2 = 0$ since $A_1A_2(S^3(V)) \subset V \cap \operatorname{Im} A_1 = V \cap \operatorname{Ker} A_1 = V \cap \operatorname{Ker} A_2$. Suppose $m > 2$. One can show that there exists $\beta \in V^G$ such that $A_2A_1(\operatorname{Im} A_2) \subset \beta^2 \operatorname{Im} A_2$. If $z \in S^k(V)$, $0 \leq k \leq 2m-1$, it follows that $A_2A_1A_2\dots(z)$ ((m+1) factors) is an element of $S^a(V)$ divisible by β^b , where $b \geq m-1 > a$, and hence is 0 . Since $S(V) = S(V)^G \sum_{k=0}^{2m-1} S^k(V)$, we obtain $A_2A_1A_2\dots = 0$ (m+1 factors). This verifies the hypothesis (iii) of Proposition 3.1 and so proves the braid relation (3.8). □

Example 3.2. Let $\varepsilon_1,\dots,\varepsilon_n$ be the standard basis of the vector space $\mathbb{Q}^n$ and let $M_{\mathbb{Z}}$ denote the lattice over $\mathbb{Z}$ spanned by

$\varepsilon_1,\ldots,\varepsilon_{n-1}$ and $\delta = \frac{1}{2}\sum_{i=1}^{n} \varepsilon_i$. Let W be the group generated by all permutations of the ε_i and all changes of the signs of the ε_i. ($M_{\mathbb{Z}}$ is the weight lattice and W the Weyl group of type B_n.) Let $\mathbb{F}_2$ be a field of characteristic 2, put $M = M_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_2$, with the action of W induced by linearity. Let $p_2,\ldots,p_n$ be the elementary symmetric functions in the ε_i of degrees $2,\ldots,n$, and put

$$q = \prod_{0 \leq i_1,\ldots,i_n \leq 1} (\delta + \Sigma\, i_s \varepsilon_s) .$$

Then $S(M)^W = \mathbb{F}_2[p_2,\ldots,p_m,q]$. However, the ideal of generalized invariants is generated by the minimal sequence $p_2,\ldots,p_n,\delta^{2^r}$, where r is defined by $n < 2^r \leq 2n$.

Example 3.3. Let $\varepsilon_1,\ldots,\varepsilon_n$ be the standard basis of $\mathbb{Z}^n$ and let $M_{\mathbb{Z}}$ denote the sublattice of $\mathbb{Z}^n$ consisting of vectors with zero sum of coordinates. Let W be the group of all permutations of the ε_i. ($M_{\mathbb{Z}}$ is the root lattice and W the Weyl group of type A_{n-1}.) Let $\mathbb{F}_p$ be a field of characteristic $p|n$, let $M = M_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$, and extend the action of W by linearity. Then the degrees of basic generalized invariants are $1,2,\ldots,\widehat{p^k},\ldots,n$, where k is such that $p^k \| n$[5]. Furthermore, the algebra $S(M)^W$ is a polynomial algebra generated by invariants of degrees 1 and 6 if $n = p = 3$, and $S(M)^W$ is not a polynomial algebra if $n = p = 5$ (R. Steinberg).

References.

1. C. Chevalley, The Betti numbers of the exceptional simple Lie groups, Proc. Int. Math. Congress II (1950), 21-24.

2. C. Chevalley, Invariants of finite groups generated by reflections, Amer. J. Math. 67 (1955), 778-782.

3. H.S.M. Coxeter, Regular polytopes, 2nd ed., Macmillan, New York, 1963.

4. V. G. Kac, K. I. Watanabe, Finite linear groups whose ring of invariants is a complete intersection, Bull. Amer. Math. Soc. 6 (1982), 221-223.

5. V. G. Kac, Torsion in cohomology of compact Lie groups and Chow rings of reductive algebraic groups, Invent. Math. (1985).

6. V. G. Kac, D. H. Peterson, Cohomology of infinite dimensional groups and their flag varieties, to appear.

7. H. Matsumura, Commutative algebra, 2nd ed., Benjamin, 1980.

8. H. Nakajima, Regular rings of invariants of unipotent groups, J. of Algebra 85 (1983), 253-286.

9. J.-P. Serre, Groupes finis d'automorphismes d'anneaux locaux réguliers, Colloq. d'Alg. ENS (1967).

10. G. C. Shephard, J. A. Todd, Finite unitary reflection groups, Can. J. Math. 6 (1954), 274-304.

11. T. A. Springer, Invariant theory, Lecture Notes in Math. 585, Springer-Verlag, 1977.

12. W. Vasconcelos, Ideals generated by R-sequences, J. Algebra 6 (1967), 303-316.

13. A. E. Zalesskii, The fixed algebra of a group generated by reflections is not always free, Arch. Math. 41 (1983), 434-437.