MULTIPLICATIVE INVARIANTS

Autor(en): **Farkas, Daniel R.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **30 (1984)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-53825

L'Enseignement Mathématique, t. 30 (1984), p. 141-157

MULTIPLICATIVE INVARIANTS

by Daniel R. FARKAS [1])

Classical invariant theory studies the action of a group G on a polynomial algebra $k[X_1, ..., X_n]$ when G restricts to a linear action on the span of $X_1, ..., X_n$. Equivalently, one starts with a finite dimensional vector space V and a group $G \subset GL(V)$. Linear automorphisms of V extend in a unique way to algebra automorphisms of the symmetric algebra on V. Thus G is a group of especially well-behaved automorphisms of an affine domain ([11]).

We will be concerned with multiplicative, rather than linear, actions. (These are also called "lattice" or "exponential" actions in the literature.) Suppose that A is a finitely generated free abelian group and G acts as a group of automorphisms of A. For $a \in A$ and $g \in G$ we shall write ${}^g a$ for the image of a. If the action is faithful, we can identify A with $\mathbf{Z}^n$ for some n and G with a subgroup of $GL(n, \mathbf{Z})$. As in the linear case, automorphisms of A can be extended to algebra automorphisms of the group algebra $k[A]$:

$${}^g(\Sigma\lambda_a a) = \Sigma\lambda_a({}^g a) .$$

We call this a "multiplicative" action.

An example might be instructive. Suppose that $k = \mathbf{C}$ and $A = \mathbf{Z}^2$. We can write the group algebra as $\mathbf{C}[X, X^{-1}, Y, Y^{-1}]$ where X and Y are algebraically independent. Suppose $g \in GL(2, \mathbf{Z})$ is the matrix $\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$. Then g is identified with the algebra automorphism which sends X to XY^{-1} and Y to $X^{-1}Y^2$. In contrast, g acts linearly on the polynomial algebra $\mathbf{C}[X, Y]$ by sending X to $X - Y$ and Y to $-X+2Y$. Notice that the linear action respects the natural grading while the multiplicative action appears more irregular.

Multiplicative actions appear inevitably in the analysis of infinite solvable groups. Suppose that a group G has a normal series with abelian factors. (It may be helpful to think of each factor as $\mathbf{Z}^n$ for some n.) If we study

[1]) Partially supported by an NSF grant.

three consecutive terms in the series, we can factor out the bottom one, obtaining normal subgroups

$$1 \subset K \subset H \subset G .$$

The application of much sophisticated ring theory to group theoretical problems begins with the observation that K (when written additively) is a $\mathbf{Z}[H]$-module. For $a = \Sigma a(h)h \in \mathbf{Z}[H]$ and $x \in K$ the action is given by

$$a * x = \Sigma a(h)\,({}^{h}x) .$$

Here ${}^{h}x$ denotes the action by conjugation, hxh^{-1}. Now suppose $g \in G$. Obviously g acts on (i.e. normalizes) K. In what sense is this action compatible with $*$? An easy calculation shows that

$${}^{g}(a*x) = \left(\Sigma a(h)ghg^{-1}\right) * ({}^{g}x) .$$

Thus we are forced to consider the action of G on $\mathbf{Z}[H]$ given by ${}^{g}(\Sigma a(h)h) = \Sigma a(h){}^{g}h$. We obtain the pleasant formula

$${}^{g}(a*x) = {}^{g}a*{}^{g}x .$$

Notice that K is actually a $\mathbf{Z}[H/K]$-module: elements of K act trivially on themselves because K is abelian. Now if it happens that $H/K \simeq \mathbf{Z}^{n}$ then G acts on $\mathbf{Z}[H/K]$ in the multiplicative fashion which is the subject of this paper.

In various special problems, more may be known about the normal series. When H is "small", K might be a cyclic $\mathbf{Z}[H/K]$-module. By studying the annihilator of K instead of K itself, one is reduced to studying G-stable ideals of $\mathbf{Z}[H/K]$ (cf. [2]). Some of the invariant theory which arises here, e.g. the determination of the full stabilizer in $GL(n, \mathbf{Z})$ of an ideal, is discussed in [6]. Similarly, one might hope to analyze how H sits inside G by finding and describing many K which are irreducible as $\mathbf{Z}[H/K]$-modules. This amounts to understanding the G-stable maximal ideals of $\mathbf{Z}[H/K]$ (cf. Lemma 5 in [9]).

This paper has five sections. In the first, we review a basic theorem of Bergman and Roseblade. It has the effect of reducing the calculation of invariants to the case of finite group actions. In particular, we observe that Hilbert's 14th problem has an affirmative solution for multiplicative actions. The second section considers Galois Theory: we look at the multiplicative action on the field of fractions, a rational function field. Sections three through five are the heart of the paper. Here we prove a Shephard-Todd-Chevalley Theorem for multiplicative invariant theory.

§ 1. The Bergman-Roseblade Theorem

We introduce some notation. Let A denote a finitely generated free abelian group. Let k be a field and have $\underline{A}$ designate an isomorphic copy of A inside the multiplicative group of some field extension of k. We will write $k[\underline{A}]$ for the k-algebra generated by $\underline{A}$ and $k(\underline{A})$ for its field of fractions. The reader is cautioned that $k[\underline{A}]$ is not the group algebra; distinct elements of $\underline{A}$ need not be linearly independent over k. (It's even possible for $\underline{A}$ to be contained in k^*.)

We will reserve the notation $k[A]$, without the underbar, for the group algebra. There is an obvious relation between the free object $k[A]$ and $k[\underline{A}]$. Indeed, the given isomorphism $A \simeq \underline{A}$ induces a k-algebra isomorphism $k[A]/P \simeq k[\underline{A}]$ where P is a prime ideal. The ideal P is "faithful with respect to A."

Suppose that G is a group which acts on A. Set

$$D = \{a \in A \mid \text{a has a finite } G\text{-orbit}\}.$$

It is sometimes called the orbital subgroup or relative finite conjugate subgroup.

We are primarily interested in a group G which acts as a group of k-automorphisms of $k[\underline{A}]$. (The slight awkwardness of language allows us to include possibly nonfaithful actions.) We say that G *acts multiplicatively* on $k[\underline{A}]$ if G stabilizes $\underline{A}$. Thus if $k[\underline{A}] = k[A]/P$ as described above, then P is a G-stable ideal under the corresponding action on $k[A]$.

The fundamental theorem in multiplicative invariant theory is Roseblade's Theorem D ([10]). Roseblade based his arguments on profound insights of G. Bergman ([3]).

Bergman-Roseblade Theorem. *Assume that* G *acts multiplicatively on* $k[\underline{A}] = k[A]/P$. *Then* $P = (P \cap k[D])k[A]$.

To understand the implications of this theorem, we take a closer look at D. Obviously D is a finitely generated abelian group. Since each generator has a finite G-orbit, D is centralized by a subgroup of finite index in G. In other words, G acts like a finite group of automorphisms when restricted to D.

It is easy to see that if a power of an element in A has a finite orbit, then so does the original element. Hence there is a splitting $A = D \times B$. (Unfortunately, there may be no choice of B which is stabilized by G.) The conclusion of the Bergman-Roseblade Theorem can be rewritten—every element in P has a unique representation $\Sigma f(b)b$ where $b \in B$ and $f(b) \in P \cap k[D]$. Thus $k[\underline{A}]$ is the group ring $(k[\underline{D}])[B]$ for a finitely generated free abelian group B.

Roseblade proves that the fixed ring $(k[\underline{A}])^G$ lies in $k[\underline{D}]$ ([10], Lemma 10). This will also be a consequence of the first lemma in the next section. In any event, it has a remarkable consequence.

THEOREM 1. *Assume that* G *is an arbitrary group acting multiplicatively on* $k[\underline{A}]$. *Then* $k[\underline{A}]^G$ *is finitely generated.*

Proof. As we have remarked, $(k[\underline{A}])^G = (k[\underline{D}])^G$. But G acts like a finite group of automorphisms on the affine algebra $k[\underline{D}]$. Noether's Theorem ([11]), states that, in this case, the algebra of invariants is a finitely generated algebra. □

This is an unexpected surprise. In contrast to the situation for linear actions, Hilbert's 14th problem holds for multiplicative actions without any restriction on the group!

The theme of the paper has emerged. A theory of invariants for multiplicative actions is ultimately a theory for finite groups.

§ 2. GALOIS THEORY

We begin this section by establishing an analogue to the "finiteness" phenomenon of the previous section, for a multiplicative action of G on $k(\underline{A})$. Notation is taken from § 1.

LEMMA 2. *Suppose that* G *acts multiplicatively on* $k(\underline{A})$. *Then* $k(\underline{A})^G \subset k(\underline{D})$.

Proof. The crucial fact is that $k(\underline{D})[B]$ is a unique factorization domain. If ${}^g f = f$ for $f \in k(\underline{A})$ then we can write $f = \alpha/\beta$ where α and β in $k(\underline{D})[B]$ have no common factors. The invariance of f becomes

$$({}^g\alpha)\beta = ({}^g\beta)\alpha \quad \text{for all} \quad g \in G .$$

Hence $\alpha \mid {}^g\alpha$ and ${}^g\alpha \mid \alpha$; we have $({}^g\alpha)\alpha^{-1}$ a unit in $k(\underline{D})[B]$. A similar result holds for β.

$${}^g\alpha = u(g)\alpha \quad \text{and} \quad {}^g\beta = w(g)\beta$$

for $u(g), w(g) \in k(\underline{D})^* \cdot B$.

It is easy to check that $u: G \to k(\underline{D})^* \cdot B$ is a crossed homomorphism. Define a "crossed" action of G on the set $k(\underline{D})^* \cdot B$ by $g \circ x = u(g)^{-1}({}^g x)$. This extends additively to an action of G on $k(\underline{D})[B]$. The defining equation for u now says $g \circ \alpha = \alpha$. Consequently, when we write out α as a non-redundant sum of elements in $k(\underline{D})^* \cdot B$,

$$\alpha = \sum_{j=1}^{N} r_j b_j \quad (b_j \text{ distinct})$$

G permutes these terms (under the crossed action). There is a subgroup H of finite index in G which fixes each term.

As we observed in the previous section, $C_G(D)$ is a subgroup of finite index in G which centralizes $k(\underline{D})$ under the ordinary action. Thus

$${}^g b_i = u(g) b_i \quad \text{for all} \quad g \in C_H(D) \quad \text{and} \quad i = 1, \ldots, N.$$

It follows that ${}^g(b_i b_j^{-1}) = b_i b_j^{-1}$ for all $g \in C_H(D)$. Since $| G: C_H(D) | < \infty$, we find that $b_i b_j^{-1} \in D$. Thus $\alpha = r_1 b_1$.

A parallel result holds for β. We conclude that $f = \xi b$ where $\xi \in k(\underline{D})^*$ and $b \in B$. Now ${}^g(\xi b) = \xi b$ for all $g \in C_H(D)$. Therefore ${}^g b = b$ for all such g, whence $b \in D \cap B = 1$. We have $f = \xi$, as desired. □

The argument we have just completed proves a bit more. We shall record the exact statement now and return to discuss it at the end of the section.

LEMMA 2′. *Suppose that G acts multiplicatively on $k(\underline{A})$. If U denotes the group of units for $k(\underline{D})[B]$ then the sequence*

$$1 \to H^1(G, U) \to H^1(G, k(\underline{A})^*)$$

is exact. □

THEOREM 3. *$k(\underline{A})^G$ is the field of fractions of $k[\underline{A}]^G$.*

Proof. According to Lemma 2, it suffices to check that $k(\underline{D})^G$ lies in the field of fractions of $k[\underline{D}]^G$. The improvement lies in the fact that G acts like a finite group of automorphisms on $k(\underline{D})$. For finite group actions, the theorem is always true ([11], Lemma 2.5.12). (Briefly, every $\alpha \in k[\underline{A}]$ divides its norm $N(\alpha) = \prod_{g \in G} ({}^g\alpha)$, so every element in $k(\underline{A})$ can be written as a fraction with an invariant denominator. If such a fraction is invariant, then its numerator must be invariant as well.) □

THEOREM 4. tr. deg. $(k(\underline{A}) \mid k(\underline{A})^G) = \operatorname{rank} A/D$.

Proof. Once again, Lemma 2 tells us that $k(\underline{A})^G = k(\underline{D})^G$. Elementary Galois Theory tells us that $k(\underline{D})$ is a finite field extension of $k(\underline{D})^G$. Hence the transcendancy degrees of $k(\underline{A}) \mid k(\underline{A})^G$ and $k(\underline{A}) \mid k(\underline{D})$ are the same.

On the other hand, the Bergman-Roseblade Theorem implies that $k(\underline{A})$ is the field of fractions of $k(\underline{D})[B]$. Since B is a free abelian group, $k(\underline{A})$ is the rational function field in rank B variables over the base field $k(\underline{D})$. Thus

$$\text{tr. deg.}\,(k(\underline{A}) \mid k(\underline{D})) = \operatorname{rank} B = \operatorname{rank} A/D. \qquad \square$$

As promised, we complete this portion of the paper with some remarks about Lemma 2′. In one sense, it measures an obstruction to the truth of Hilbert's Theorem 90 for multiplicative actions. Of course there is an intimate connection between invariant theory and crossed homomorphisms. Suppose that Λ is any k-algebra and G acts as a group of k-algebra automorphisms of Λ. If $\lambda \in \operatorname{Hom}(G, k^*)$ then a semi-invariant with weight λ is a nonzero element f in Λ such that ${}^g f = \lambda(g) f$ for all $g \in G$. The vanishing of $H^1(G, k(\underline{A})^*)$ is a statement about the triviality of semi-invariants. To be more precise, we add a condition which separates k and $\underline{A}$.

PROPOSITION 5. *Assume that* $k^* \cap \underline{A} = 1$. *Then*

$$1 \to \operatorname{Hom}(G/C_G(D), k^*) \to \operatorname{Hom}(G, k^*) \to H^1(G, k(\underline{A})^*)$$

is exact.

Proof. Let $M = \ker(\operatorname{Hom}(G, k^*) \to H^1(G, k(\underline{A})^*))$. The problem is to prove that $M = \{\lambda \in \operatorname{Hom}(G, k^*) \mid \lambda(C_G(D)) = 1\}$.

First suppose that $\lambda \in M$. Then there is a nonzero $f \in k(\underline{A})$ such that ${}^g f = \lambda(g) f$ for all $g \in G$. By Lemma 2′, we can write $f = \xi b$ for some $\xi \in k(\underline{D})^*$ and $b \in B$. If $g \in C_G(D)$ then ${}^g b = \lambda(g) b$ which, in turn, implies that $\lambda(g) = ({}^g b) b^{-1} \in k^* \cap \underline{A}$. We conclude that λ vanishes on $C_G(D)$.

For the opposite inclusion, assume that $\lambda(C_G(D)) = 1$. Then $\lambda \in \operatorname{Hom}(\mathscr{G}, k^*)$ where $\mathscr{G} = G/C_G(D)$ is a finite group of automorphisms of $k(\underline{D})$. Hilbert's Theorem 90 now applies: $H^1(\mathscr{G}, k(\underline{D})^*) = 1$. Certainly the image of $\operatorname{Hom}(\mathscr{G}, k^*)$ in $H^1(\mathscr{G}, k(\underline{D})^*)$ is trivial. In other words, there is an $\eta \in k(\underline{D})^*$ such that ${}^t\eta = \lambda(t)\eta$ for $t \in \mathscr{G}$. Clearly ${}^g\eta = \lambda(g)\eta$ for $g \in G$. Thus λ vanishes in $H^1(G, k(\underline{A})^*)$. $\square$

A similar application of Lemma 2′ will yield the analogue of Theorem 3 for semi-invariants: if $k^* \cap \underline{A} = 1$ then

$$k(\underline{A})^G_\lambda = (k[\underline{A}]^G)^{-1}(k[\underline{A}]^G_\lambda).$$

Recall that $G/C_G(D)$ is a finite group. Hence $\mathrm{Hom}(G/C_G(D), k^*)$ is finite. Consequently, when $\mathrm{Hom}(G, k^*)$ is infinite the proposition implies that $H^1(G, k(\underline{A})^*) \neq 1$. It is quite plausible (under the assumption $k^* \cap \underline{A} = 1$) that $H^1(G, k(\underline{A})^*)$ vanishes if and only if G is finite.

The extra bothersome assumption is vacuous in the case of group algebras. One can read off the following observation from Lemma 2′.

PROPOSITION 6. *Assume that* $D = 1$. *Then*

$$1 \to \mathrm{Hom}(G, k^*) \times H^1(G, A) \to H^1(G, k(A)^*) \quad \textit{is exact}. \qquad \square$$

I have been unable to determine if the injection given by the proposition always splits. Here is one situation where it does.

PROPOSITION 7. *Suppose that* A *can be fully ordered so that* G *acts as a group of order automorphisms of* A. *Then the natural map*

$$H^1(G, k^* \cdot A) \to H^1(G, k(A)^*)$$

splits.

Proof. Let $V: k[A]\backslash\{0\} \to k^* \cdot A$ be the function which sends an element to its "lowest term" with respect to the ordering. The usual degree argument which shows that a polynomial ring is a domain, establishes that V is multiplicative. Since elements of G act monotonically, V is a map of (multiplicative) G-modules. It is not difficult to check that V extends to a multiplicative G-map from $k(A)^*$ to $k^* \cdot A$.

Obviously $k^* \cdot A \to k(A)^* \xrightarrow{V} k^* \cdot A$ provides the necessary splitting. $\square$

The hypothesis of Proposition 7 is very restrictive, even for an infinite cyclic group G. We leave the following long exercise to the reader. A matrix in $GL(n, \mathbf{Z})$ is order preserving for some ordering on $\mathbf{Z}^n$ and only if each rational irreducible factor of its characteristic polynomial has a positive real root.

§ 3. THE SHEPHARD-TODD-CHEVALLEY THEOREM

Recall that a matrix in $GL(n, \mathbf{C})$ is a pseudo-reflection if it has finite order and 1 is an eigenvalue of multiplicity $n - 1$. The remaining eigenvalue for a pseudo-reflection must be a root of unity; when it is -1 we call the matrix a reflection. Notice that every pseudo-reflection in $GL(n, \mathbf{Z})$ must be a reflection. A pseudo-reflection group (resp. reflection group) is a finite group generated by pseudo-reflections (resp. reflections). The classical result is the

SHEPHARD-TODD-CHEVALLEY THEOREM (cf. [11], Theorem 4.2.5). *Suppose that G is a finite group of automorphisms of $\mathbf{C}[X_1, ..., X_n]$ which acts linearly. Then $\mathbf{C}[X_1, ..., X_n]^G$ is a polynomial ring if and only if G is a pseudo-reflection group.*

The major theorem of this section is one direction of the STC Theorem for multiplicative actions. Namely,

THEOREM 8. *Suppose that $G \subset GL(n, \mathbf{Z})$ is a finite group of automorphisms of $A \simeq \mathbf{Z}^n$. If $\mathbf{C}[A]^G$ is a polynomial ring then G is a reflection group.*

This theorem is deduced from the STC Theorem via a connection between abelian group algebras and polynomial rings which goes back to the pioneers of infinite group theory. From now on A will be the free abelian group on n generators. Let V be the n-dimensional complex vector space $\mathbf{C} \otimes_{\mathbf{Z}} A$. If x is in A we shall write $\bar{x} = 1 \otimes x$ in V. The symmetric algebra on V will be denoted $\mathbf{C}[V]$. (We warn the reader of our primitive tendencies; $\mathbf{C}[V]$ is not the algebra of polynomial functions on V.) Both $\mathbf{C}[A]$ and $\mathbf{C}[V]$ have canonical augmentations. In the former case the augmentation ideal ω is the ideal generated by $\{x - 1 \mid x \in A\}$. In the latter, ω is the ideal generated by vectors in V. Let $\mathbf{C}[A]^\wedge$ and $\mathbf{C}[V]^\wedge$ be the respective ω-adic completions. The exponential function from A into $\mathbf{C}[V]^\wedge$ given by

$$\exp(x) = \sum_{j=0}^{\infty} (\bar{x}^j)/j!$$

is well-defined. It extends by linearity and then continuity to a $\mathbf{C}$-algebra map $E\colon \mathbf{C}[A]^\wedge \to \mathbf{C}[V]^\wedge$. In fact, E is an isomorphism. (The map back extends the logarithm.)

The effect of this identification on automorphisms was first exploited in [1]. A matrix $g \in GL(A)$ induces an automorphism γ on $\mathbf{C}[A]^\wedge$. What is the automorphism after "translating" by E? The following calculation of $E\gamma E^{-1}$ on x can be checked in detail on the matrix level:

$$(E\gamma E^{-1})(\bar{x}) = E\gamma E^{-1}(\log E(x)) = E(\log {}^g x)$$
$$= E(g(\log x)) = g(\log E(x)) = g(\bar{x}) .$$

LINEARIZATION THEOREM. *Let G be a group of automorphisms of A, regarded in $GL(n, \mathbf{Z})$. Exponentiation extends to an algebra isomorphism $E: \mathbf{C}[A]^\wedge \to \mathbf{C}[V]^\wedge$. Moreover, the multiplicative action of G (extended by continuity) on $\mathbf{C}[A]^\wedge$ induces an action on $\mathbf{C}[V]^\wedge$ which is the extension (by continuity) of the linear action of G on $\mathbf{C}[V]$.* □

With this tool in hand, the proof of Theorem 8 amounts to carefully keeping track of a myriad of completions and then getting rid of them. The calculations are somewhat clearer in the abstract. So let S be a $\mathbf{C}$-algebra and let G be a finite group of automorphisms of S. The averaging or Reynolds operator which sends S to the fixed ring S^G is given by

$$\operatorname{av}(c) = \frac{1}{|G|} \sum_{g \in G} {}^g c$$

The function av is an idempotent S^G-module map.

LEMMA 9. *Suppose that S is a commutative noetherian $\mathbf{C}$-algebra and I is a G-stable maximal ideal. Then there is a positive integer f such that*

$$I^{ft} \cap S^G \subset (I \cap S^G)^t \subset I^t \cap S^G \quad \textit{for} \quad t = 1, 2, \ldots .$$

Proof. The second inclusion is obvious. Set $J = I \cap S^G$. We first prove that I is the only prime ideal lying over JS.

Indeed, suppose P is a prime ideal of S containing J. If $a \in I$ then $\prod_{g \in G} {}^g a \in I \cap S^G \subset P$. By primality there is some $g \in G$ with $a \in {}^g P \cap I$. Consequently, $I = \bigcup_{g \in G} ({}^g P \cap I)$, a union of complex subspaces. At least one of these subspaces is not proper: there is an $h \in G$ such that $I = {}^h P \cap I$. Therefore $I = {}^{h^{-1}} I \subset P$. Maximality implies $I = P$, as required.

The prime radical of S/JS is the image of I. But the prime radical is nil and nil ideals in a noetherian ring are nilpotent. Hence there is a positive integer f such that $I^f \subset JS$.

We have established, so far, that $I^{ft} \subset J^t S$ for all t. Intersect each side of the inclusion S^G and apply the averaging operator.

$$I^{ft} \cap S^G = \operatorname{av}(I^{ft} \cap S^G) = \operatorname{av}(J^t S \cap S^G) \subset \operatorname{av}(J^t S) = J^t \operatorname{av}(S)$$

We have obtained the necessary inclusion:

$$I^{ft} \cap S^G \subset J^t = (I \cap S^G)^t .$$ □

LEMMA 10. *Suppose that S has a filtration $S = S_0 \supset S_1 \supset S_2 \supset \ldots$ such that each S_j is G-stable and $\cap S_j = 0$. Then* $(S^\wedge)^G = (S^G)^\wedge$. (Here

$S^\wedge$ denotes the completion of S with respect to the given filtration and $(S^G)^\wedge$ means the completion of S^G for the "relative" filtration $S_j \cap S^G$.)

Proof. There is an obvious injection $(S^G)^\wedge \to S^\wedge$, where the topology on $(S^G)^\wedge$ coincides with the relative topology on its image. Notice that the action of G on S extends continuously to an action on $S^\wedge$: if $a_m \to a$ then ${}^g a_m \to {}^g a$. It follows that $(S^G)^\wedge \subset (S^\wedge)^G$.

Suppose $b \in (S^\wedge)^G$. Choose a sequence $b_m \in S$ such that $b_m \to b$. Then $\mathrm{av}(b_m) \to \mathrm{av}(b)$ and $\mathrm{av}(b) = b$. Hence $b \in (S^G)^\wedge$. □

LEMMA 11. *Suppose that* k *is a field and* $\Phi: k[T_1, ..., T_n] \to k$ *is a* k*-algebra homomorphism. Then there is a change of variables,*

$$k[T_1, ..., T_n] = k[T'_1, ..., T'_n],$$

so that $\ker \Phi = (T'_1, ..., T'_n)$.

Proof. Consider the automorphism induced by sending each T_j to $T'_j = T_j - \Phi(T_j)$. □

The next lemma is undoubtedly routine for the expert in commutative algebra. Rather than interrupt the flow of the narrative, we will state it now and then relegate a sketchy proof to the appendix.

DECOMPLETION LEMMA. *Let* k *be a field and suppose* $R = R_{(0)} \oplus R_{(1)} \oplus \ldots$ *is a graded* k*-algebra with* $R_{(0)} = k$. *If* $\hat{R}$ *(its completion with respect to the grade filtration) is algebra isomorphic to a power series ring* $k[[T_1, ..., T_n]]$ *then* R *is isomorphic to a polynomial ring in* n *homogeneous variables.*

Proof of Theorem 8 that if $\mathbf{C}[A]^G$ is a polynomial ring then G is a reflection group: According to Lemma 10, $(\mathbf{C}[A]^\wedge)^G = (\mathbf{C}[A]^G)^\wedge$. Here $(\mathbf{C}[A]^G)^\wedge$ is the completion of $\mathbf{C}[A]^G$ with respect to the filtration $\omega^t \cap \mathbf{C}[A]^G$. A straightforward Cauchy sequence argument in conjunction with Lemma 9 shows that $(\mathbf{C}[A]^G)^\wedge$ is also the $(\omega \cap \mathbf{C}[A]^G)$-adic completion. Now $\mathbf{C}[A]^G$ is a polynomial ring in $n = \mathrm{rank} A$ variables and $\omega \cap \mathbf{C}[A]^G$ is a codimension one ideal. By Lemma 11, the $(\omega \cap \mathbf{C}[A]^G)$-adic completion of $\mathbf{C}[A]^G$ is isomorphic to the power series ring $\mathbf{C}[[T_1, ..., T_n]]$.

In summary, $(\mathbf{C}[A]^\wedge)^G \simeq \mathbf{C}[[T_1, ..., T_n]]$. Next, apply the isomorphism E and use Lemma 10 for the symmetric algebra. We find that $(\mathbf{C}[V]^G)^\wedge \simeq \mathbf{C}[[T_1, ..., T_n]]$. This time, $\mathbf{C}[V]^G$ is a *graded* algebra under the grading inherited from $\mathbf{C}[V]$ and its completion is with respect to the grade filtration.

We are in the situation of the Decompletion Lemma for $\mathbf{C}[V]^G = R$. Thus $\mathbf{C}[V]^G$ is a polynomial ring in n homogeneous variables. Our theorem now follows from the STC Theorem. □

It is possible to object to the appropriateness of proving a theorem which determines when the invariants for a group algebra comprise a polynomial algebra. After all, the most well-behaved group is the group of order one and its fixed ring is the group algebra we began with. Let's say that a $\mathbf{C}$-algebra is an *extended polynomial ring* if it contains algebraically independent elements $U_1, ..., U_m, T_1, ..., T_n$ such that the algebra is isomorphic to $\mathbf{C}[U_1, U_1^{-1}, ..., U_m, U_m^{-1}, T_1, ..., T_n]$. Equivalently, an extended polynomial ring has the form $\mathbf{C}[U] \otimes_{\mathbf{C}} \mathbf{C}[T_1, ..., T_n]$ where U is a finitely generated free abelian group. Once the generators U_i and T_j are distinguished, its augmentation ideal ω is the ideal generated by $U_1 - 1, ..., U_m - 1, T_1, ..., T_n$.

The theorem we have proved can be adapted to prove the "correct" result.

THEOREM 8^+. *Suppose G is a finite group acting faithfully and multiplicatively on $\mathbf{C}[A]$. If $\mathbf{C}[A]^G$ is an extended polynomial ring then G is a reflection group.*

Proof. We follow the argument a few lines up. It is still true that $(\mathbf{C}[A]^\wedge)^G$ is the $(\omega \cap \mathbf{C}[A]^G)$-adic completion of $\mathbf{C}[A]^G$. This time $\omega \cap \mathbf{C}[A]^G$ is a codimension one ideal in the extended polynomial ring $\mathbf{C}[A]^G$. We need Lemma 11^+: if

$$\Phi: k[U_1^{\pm 1}, ..., U_m^{\pm 1}, T_1, ..., T_n] \to k$$

is an algebra homomorphism then there is a change of variables so that $\ker\Phi$ becomes the augmentation ideal. (Indeed, define $U'_j = \Phi(U_j)^{-1} U_j$ and $T'_j = T_j - \Phi(T_j)$.)

What is the completion of an extended polynomial ring with respect to powers of its augmentation ideal? Topological abstract nonsense shows that it coincides with $\mathbf{C}[U]^\wedge[[T_1, ..., T_n]]$ where $\mathbf{C}[U]^\wedge$ is the completion of the group algebra with respect to the $(U_1 - 1, ..., U_m - 1)$-adic topology. But the linearizing E-isomorphism exhibits $\mathbf{C}[U]^\wedge$ as a power series ring in $\operatorname{rank} U$ variables. In summary, the augmentation-adic completion of an extended polynomial ring is also a power series ring.

From here on, the previous argument can be carried over verbatim. □

It is much more difficult to decide when $\mathbf{C}(A)^G$ is a rational function field. The little that is known is surveyed in [7].

§ 4. Appendix

$R = R_{(0)} \oplus R_{(1)} \oplus \ldots$ is a graded k-algebra with $R_{(0)} = k$. Let $\mathfrak{m}$ be the maximal ideal $\sum_{i=1}^{\infty} R_{(i)}$. We assume that $\hat{R}$ is a power series ring in finitely many variables. Obviously $\hat{\mathfrak{m}}$ corresponds to the unique maximal ideal of the power series ring, whence $\hat{R}/\hat{\mathfrak{m}}^d$ is always finite dimensional. Since $\hat{\mathfrak{m}}^d$ is homogeneous, some tail $\prod_{?}^{\infty} R_{(i)}$ must then lie in $\hat{\mathfrak{m}}^d$. It follows that the graded algebra of R for the $\mathfrak{m}$-adic filtration is isomorphic to the graded algebra of $\hat{R}$ for the $\hat{\mathfrak{m}}$-adic filtration. The power series assumption implies that the latter is simply a polynomial ring with the standard grading.

Clearly $\mathfrak{m}^2 \subset \sum_{j=2}^{\infty} R_{(j)}$. Hence $R_{(1)}$ injects into $\mathfrak{m}/\mathfrak{m}^2$. Choose a basis for $R_{(1)}$ over k and extend it to a list of homogeneous elements $x_1, \ldots, x_n$ in $\mathfrak{m}$ whose images constitute a basis for $\mathfrak{m}/\mathfrak{m}^2$. It is generally true for any commutative k-algebra R that when $R/\mathfrak{m} = k$ and when the associated graded ring for the $\mathfrak{m}$-adic filtration is the symmetric algebra on $\mathfrak{m}/\mathfrak{m}^2$, that any basis for $\mathfrak{m}/\mathfrak{m}^2$ pulls back to a set of algebraically independent elements in R. In particular, $x_1, \ldots, x_n$ are algebraically independent.

We use the given grading on R to prove that $R = k[x_1, \ldots, x_n]$. Vacuously, $R_{(0)} \subset k[x_1, \ldots, x_n]$. We have chosen the x_i so that $R_{(1)}$ lies in their span, so $R_{(1)} \subset k[x_1, \ldots, x_n]$. Assume, inductively, that $d \geqslant 1$ and $R_{(s)} \subset k[x_1, \ldots, x_n]$ for all $s \leqslant d$. If $y \in R_{(d+1)}$ then

$$y = \Sigma \lambda_i x_i + \Sigma u_j v_j$$

for some $\lambda_i \in k$ and u_j, $v_j \in \mathfrak{m}$. Without loss of generality u_j and v_j are homogeneous and all the x_i and $u_j v_j$ which appear in the formula lie in $\bigcup_{t=1}^{d+1} R_{(t)}$. This can only happen when u_j and v_j are in $R_{(s)}$ for some $s \leqslant d$. By induction, u_j and v_j are elements of $k[x_1, \ldots, x_n]$. Therefore $y \in k[x_1, \ldots, x_n]$.

§ 5. Weyl Groups

It seems to be-part of the folklore for Lie theory that the converse of Theorem 8 fails to be true (cf. [4] VI§ 3 Ex. 2). Rather than being dead-ends, these examples serve as inspiration: the machinery of root systems will allow us to determine the correct necessary and sufficient conditions for a multiplicative Shephard-Todd-Chevalley analogue. For the most part, we will follow the notation in [8].

Suppose that V is an n-dimensional complex vector space and $G \subset GL(V)$. By a G-lattice we mean a lattice in V (of rank n) which is invariant under the action of G. The G-lattice A is effective if zero is the only element fixed by all members of G. Notice that A is effective if and only if the units of $\mathbf{C}[A]^G$ are precisely the nonzero elements of $\mathbf{C}$.

PROPOSITION 12. *Let A be an effective G-lattice. If G is a finite group generated by reflections then*

(i) *there is a reduced root system Φ lying in A so that G is the Weyl group for Φ, and*

(ii) *A (considered inside V) lies between the root lattice for Φ and the weight lattice.*

Proof. Endow V with an inner product which makes members of G orthogonal transformations. If σ is a reflection in G and $a \in A$ is such that $a \neq \sigma(a)$ then $a - \sigma(a) \neq 0$ and $\sigma(a-\sigma(a)) = -(a-\sigma(a))$. Thus $\{b \in A \mid \sigma(b) = -b\}$ is an infinite cyclic subgroup of A. Its two possible generators, a_σ and $-a_\sigma$, are the nonzero vectors of smallest length in A which are "reflected" by σ. It is not difficult to check that $\Phi = \{\pm a_\sigma \mid \sigma \text{ is a reflection in } G\}$ is a root system, whence G is its Weyl group. Moreover, if $x \in A$ and $\alpha = \pm a_\sigma \in \Phi$ then $\sigma(x) \in A$. Thus $x - \frac{2(x, \alpha)}{(\alpha, \alpha)}\alpha \in A$. Now $\frac{2(x, \alpha)}{(\alpha, \alpha)}\alpha \in A$ implies that $\frac{2(x, \alpha)}{(\alpha, \alpha)}$ is an integer. This is just the statement that x is a weight. □

Although we have "located" the effective G-lattices, there are still quite a few of them: every lattice between the root lattice and the weight lattice is invariant under G. On the positive side, it turns out that the group algebra of the weight lattice has well-behaved invariants.

THEOREM ([4], VI § 3.4). *Let G be a Weyl group and let Λ be its weight lattice. Then $\mathbf{C}[\Lambda]^G$ is a polynomial ring.* □

This theorem of Bourbaki can be generalized just enough to suggest its own converse. Fix a root system with base Δ. Let Λ_r and Λ denote the root lattice and weight respectively and let $w_1, \ldots, w_n$ be the fundamental dominant weights. Then Λ^+ is the collection of dominant weights: the non-negative integer combinations of $w_1, \ldots, w_n$. Write W for the Weyl group.

In [5], we introduced the notion of *stretched weight lattice* for a root system. It is a W-lattice lying between Λ_r and Λ which has a basis of the form $r_1 w_1, r_2 w_2, \ldots, r_n w_n$ for positive integers $r_1, \ldots, r_n$. A stretched weight lattice can always be built up from ordinary weight lattices and certain root lattices ([5]). More unexpectedly, we found an abstract characterization. Suppose G is a finite subgroup of $GL(n, \mathbf{Z})$; then the corresponding action on $\mathbf{Z}^n$ has the non-negative "quadrant" as fundamental domain (in Bourbaki's strong sense) if and only if G is a Weyl group and $\mathbf{Z}^n$ is isomorphic to a stretched weight lattice for G.

To talk about the group algebra $\mathbf{C}[\Lambda]$, we will have to switch from additive to multiplicative notation for elements of Λ. If we think of λ as a weight then λ^* will be its image in $\mathbf{C}[\Lambda]$, e.g. $(\lambda_1 - \lambda_2)^* = (\lambda_1^*)(\lambda_2^*)^{-1}$.

For $\lambda \in \Lambda$ we set $X(\lambda) = (\text{constant}) \cdot \text{av}(\lambda^*)$ where the normalizing constant is chosen so that each element of Λ appears with coefficient 0 or 1 in $X(\lambda)$. Using this notation, we state the appropriate form of Bourbaki's Theorem. (The proof carries over verbatim from [4].)

THEOREM 13. *If S is a stretched weight lattice with basis $r_1 w_1, \ldots, r_n w_n$ then*

$$\mathbf{C}[S]^W = \mathbf{C}[X(r_1 w_1), \ldots, X(r_n w_n)] .$$

Moreover, $X(r_1 w_1), \ldots, X(r_n w_n)$ are algebraically independent. □

We shall frequently use the consequence that $X(w_1), \ldots, X(w_n)$ are irreducible elements of the unique factorization domain $\mathbf{C}[\Lambda]^W$.

For the rest of this paper, M will be a W-lattice with

$$\Lambda_r \subset M \subset \Lambda .$$

LEMMA 14. *Suppose $\lambda_1, \ldots, \lambda_t$ are (not necessarily distinct) dominant weights. If $\lambda_1 + \ldots + \lambda_t \in M$ then $(g_1 \cdot \lambda_1) + \ldots + (g_t \cdot \lambda_t) \in M$ for all choices $g_1, \ldots, g_t \in W$.*

Proof. For $\alpha \in \Delta$ let σ_α denote reflection in the hyperplane perpendicular to α. Then $\sigma_\alpha(\lambda_j) = \lambda_j - < \lambda_j, \alpha > \alpha$. The definition of "weight" implies that $< \lambda_j, \alpha >$ is an integer. Thus

$$\sigma_\alpha(\lambda_j) \equiv \lambda_j \,(\text{mod } \Lambda_r)$$

and so,

$$\sigma_\alpha(\lambda_j) \equiv \lambda_j \,(\text{mod } M).$$

Now W is generated by $\{\sigma_\alpha \mid \alpha \in \Delta\}$. An easy induction on the length of $g \in W$ as a word in the generators yields

$$g(\lambda_j) \equiv \lambda_j \,(\text{mod } M).$$

Hence

$$\sum_{j=1}^{t} g_j(\lambda_j) \equiv \sum_{j=1}^{t} \lambda_j \,(\text{mod } M). \qquad \square$$

LEMMA 15. *Suppose* $\lambda_1, \ldots, \lambda_t$ *are (not necessarily distinct) dominant weights. If* $\lambda_1 + \ldots + \lambda_t \in M$ *then*

$$X(\lambda_1)X(\lambda_2) \cdots X(\lambda_t) \in \mathbf{C}[M]^W.$$

Proof. A typical element of Λ in the support of $X(\lambda_1) \cdots X(\lambda_t)$ has the form $(g_1(\lambda_1)+\ldots+g_t(\lambda_t))^*$ where $g_1, \ldots, g_t \in W$. According to Lemma 14, $\Sigma g_j(\lambda_j) \in M$. Thus

$$X(\lambda_1)X(\lambda_2) \cdots X(\lambda_t) \in \mathbf{C}[M] \cap \mathbf{C}[\Lambda]^W. \qquad \square$$

We say that an element $w \in M \cap \Lambda^+$ is *M-indecomposable* if it cannot be written as a sum of two nonzero elements of $M \cap \Lambda^+$. Clearly, every element of $M \cap \Lambda^+$ is a sum of M-indecomposable elements.

THEOREM 16. *The following statements are equivalent:*

(i) M *is a stretched weight lattice for* W.

(ii) $\mathbf{C}[M]^W$ *is a polynomial ring.*

(iii) $\mathbf{C}[M]^W$ *is a UFD.*

Proof. (i) $\Rightarrow$ (ii) is Theorem 13 and (ii) $\Rightarrow$ (iii) is classical. Thus we assume that $\mathbf{C}[M]^W$ is a *UFD* and prove (i).

Suppose $\sum_{j=1}^{n} a_j w_j$ is M-indecomposable. According to Lemma 15,

$$Y = X(w_1)^{a_1} X(w_2)^{a_2} \cdots X(w_n)^{a_n}$$

is an element of $\mathbf{C}[M]^W$. Every coefficient appearing in $X(w_j)$ is 1; hence any subproduct

$$X(w_1)^{b_1} X(w_2)^{b_2} \cdots X(w_n)^{b_n}$$

with $0 \leqslant b_j \leqslant a_j$ contains $(\sum_{j=1}^{n} b_j w_j)^*$ in its support. If Y factors in $\mathbf{C}[M]^W$ then each factor is one such subproduct by the *UFD* property of $\mathbf{C}[\Lambda]^W$. Therefore, a factoring provides b_j for $j = 1, ..., n$ such that $0 \leqslant b_j \leqslant a_j$, not all $b_j = a_j$, and both $\Sigma b_j w_j$ and $\Sigma(a_j - b_j)w_j$ lie in M. This contradicts the M-indecomposability of $\Sigma a_j w_j$. In summary, Y is an irreducible element in $\mathbf{C}[M]^W$.

Let d be the index of M in Λ. Then $dw_j \in M$ for each fundamental dominant weight w_j. Again, Lemma 15 yields

$$X(w_j)^d \in \mathbf{C}[M]^W \quad \text{for} \quad j = 1, ..., n\,.$$

Consider the equation

$$Y^d = [X(w_1)^d]^{a_1}[X(w_2)^d]^{a_2} \cdots [X(w_n)^d]^{a_n}$$

inside $\mathbf{C}[M]^W$. Since Y is irreducible, $Y \mid X(w_k)^d$ for some k. Interpret this in $\mathbf{C}[\Lambda]^W$ and use unique factorization there: $Y = X(w_k)^{a_k}$. That is, the M-indecomposable weights all have the form $a_k w_k$.

If $a_k w_k$ and $a'_k w_k$ lie in M, so does $GCD(a_k, a'_k)w_k$. But $GCD(a_k, a'_k)$ divides both a_k and a'_k. By indecomposability, there are no such repeats:

$$r_1 w_1, ..., r_n w_n \qquad (r_j > 0 \text{ an integer})$$

is a complete list of the M-indecomposable elements. (Notice that some positive integer multiple of each w_j *must* be M-indecomposable.) They are clearly linearly independent over $\mathbf{Z}$. The argument is completed by showing that they span M. Suppose $\sum_{i=1}^{n} c_i w_i \in M$. Choose a large positive integer N such that $\frac{c_i}{r_i} \leqslant N$ for $i = 1, ..., n$. Since $r_i w_i \in M$ we have $N(\sum_{i=1}^{n} r_i w_i) \in M$. Thus $\sum_{i=1}^{n} (Nr_i - c_i)w_i \in M$. Since $Nr_i - c_i \geqslant 0$,

$$\sum_{i=1}^{n} (Nr_i - c_i)w_i \in M \cap \Lambda^+\,.$$

Now every member of $M \cap \Lambda^*$ is a sum of M-indecomposable elements. Solve for $\Sigma c_i w_i$. □

Finally, we can put together Theorem 8, Proposition 12, and Theorem 16. We cite the fact that a reflection group may appear as the Weyl group for more than one root system. By replacing certain component root systems of type B_n with those of type C_n, every stretched weight lattice over a given reflection group becomes isomorphic, as an abstract module, to some ordinary weight lattice. (See § 1 and the "note added in proof" of [5].)

MAIN THEOREM. *Assume A is a* **Z***-lattice and $G \subset GL(A)$ is a finite group. Then* $\mathbf{C}[A]^G$ *is a polynomial ring if and only if G is a reflection group and, for some choice of root system, it becomes a Weyl group with A as its weight lattice.*

REFERENCES

[1] AUSLANDER, L. and G. BAUMSLAG. Automorphism groups of finitely generated nilpotent groups. *Bull. Amer. Math. Soc. 73* (1967), 716-717.

[2] BACHMUTH, S., G. BAUMSLAG, J. DYER and H. Y. MOCHIZUKI. Automorphism groups of 2-generator metabelian groups. *Preprint.*

[3] BERGMAN, G. M. The logarithmic limit-set of an algebraic variety. *Trans. Amer. Math. Soc. 157* (1971), 459-469.

[4] BOURBAKI, N. *Groupes et Algèbres de Lie*, IV, V, VI. Hermann, Paris, 1968.

[5] FARKAS, D. R. The stretched weight lattices of a Weyl group. *Preprint.*

[6] —— and R. L. SNIDER. Arithmeticity of stabilizers of ideals in group rings. To appear in *Inventiones.*

[7] FORMANEK, E. Rational function fields—Noether's problem and related questions. *Preprint.*

[8] HUMPHREYS, J. E. *Introduction to Lie Algebras and Representation Theory.* Grad. Texts in Math. 9 (1972), Springer-Verlag, New York.

[9] ROSEBLADE, J. E. Group rings of polycyclic groups. *J. Pure Appl. Alg. 3* (1973), 307-328.

[10] —— Prime ideals in group rings of polycyclic groups. *Proc. London Math. Soc. (3) 36* (1978), 385-447.

[11] SPRINGER, T. A. *Invariant Theory.* Lecture notes in math. #585 (1977), Springer-Verlag, Berlin.

(Reçu le 14 décembre 1983)

Daniel R. Farkas

Virginia Polytechnic Institute
and State University
Blacksburg, VA 24061
USA

NOTE ADDED IN PROOF: As occasionally happens when a mathematician wanders from his area of expertise, he re-invents the wheel. The appendix (§ 4) can be eliminated by invoking a theorem of Serre [B] to the effect that the fixed ring of a suitably nice regular local ring under the action of a finite group is also regular local if and only if the group acts as a pseudo-reflection group on the tangent space of the original local ring. The fifth section is, to a large extent, implicit in work of Steinberg [C]. A statement closer to mine can be found in [A].

[A] RICHARDSON, R. W. Orbits, invariants and representations. *Invent. math. 66* (1982), 287-312.

[B] SERRE, J.-P. Groupes finis d'automorphismes d'anneaux locaux réguliers. *Colloque d'Algèbre Exp. 8*, Ecole Normale Supérieure de Jeunes Filles (1968).

[C] STEINBERG, R. On a theorem of Pittie. *Topology 14* (1975), 173-177.

vide-leer-empty