TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 310, Number 2, December 1988

GROUPS ACTING ON AFFINE ALGEBRAS

D. R. FARKAS

ABSTRACT. General actions of groups on commutative affine domains are studied. We prove a finiteness theorem for orbits of ideals and an ergodic theorem inspired by results from the theories of group algebras and universal enveloping algebras.

This paper began as a reconsideration of "ergodic" theorems in the theory of group algebras ([2], [3], [4]). The philosophy of these results is the following. If A is a lattice (i.e., a group isomorphic to $\mathbb{Z}^n$) and G is a group of automorphisms of A then G acts on the maximal spectrum of the group algebra $k[A]$. Thus G mixes up the points on a torus. The ergodic theorems study the connections between the original action on A and the nature of orbits on the torus.

Although one can obtain many analogues to classical theorems in ergodic theory in this way, the program is ultimately insufficient. One ought not confine the study to orbits of maximal ideals; after all, there are likely to be G-invariant closed subsets of the torus which are not finite unions of closures of point orbits. To account for these more complicated situations, we introduce a simple-minded but new notion to the theory of groups acting on rings. It will turn out that this concept sheds light on old theorems concerning enveloping algebras of Lie algebras and suggests new problems in commutative algebra.

For the remainder of the paper, k denotes a commutative field and R is a commutative affine k-algebra. Assume G is a group of k-automorphisms of R. We are particularly interested in the case that G is infinite. The role played by maximal ideals above is taken over by G-variant prime ideals. A prime ideal P of R is *G-variant* provided that P is maximal among all ideals Q such that

$$\bigcap_{g\in G} {}^gQ = \bigcap_{g\in G} {}^gP.$$

In other words, P is the "farthest from invariant" ideal with the property that the intersection of its conjugates is a certain invariant ideal. To indicate the direction of this paper, we can now state two theorems.

THEOREM. *A prime ideal P is both G-variant and G-invariant if and only if G acts like a finite group on R/P.*

We shall see that this theorem can be reformulated in the following pleasing way: If R is a domain and every ideal has a finite orbit then G is finite. The second theorem we establish is related to Dixmier's problem of the "existence of generic ideals" for enveloping algebras [11].

Received by the editors January 14, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 13B10; Secondary 14L30, 17B35.

THEOREM. *Assume k is an uncountable field. If P is a G-variant prime ideal of R and $I = \bigcap_{g\in G} {}^gP$ is prime then*

$$d(P) = \text{tr.deg.}_k Q(R/I)^G.$$

Here $d(P)$ is the Krull dimension of R/P and $Q(R/I)$ is the field of fractions of R/I. Some readers will recognize that this is an assertion about hearts of primes.

It is fair to ask how the mathematics in this paper relates to classical invariant theory. Traditionally. the groups acting on affine algebras which have been studied act "geometrically" or "rationally" [**8**]. Indeed, Moeglin and Rentschler prove a version of the second theorem [**7**] for rational actions on a class of noncommutative, noetherian, affine algebras. The novelty of this paper is that it exhibits genuine theorems about arbitrary actions. The program begun here ought to relate to research about the automorphism group of a polynomial ring in several variables. Certainly it would be helpful to know the status of the Burnside Problem (see Lemma 11) and the Tits Alternative for groups of automorphisms of affine domains.

In preparing this article, I enjoyed many stimulating conversations with colleagues. I thank Hyman Bass, Hanspeter Kraft, Claudio Procesi, and, especially, Peter Linnell for their attention and helpful observations.

1. Celestial algebra. We remind the reader that R is a commutative affine k-algebra and G is a group of k-automorphisms of R. (We note, however, that the results of this section hold generally in noetherian rings.)

If J is an ideal of R, we shall refer to $\bigcap_{g\in G} {}^gJ$ as the orb of J. When I is a G-invariant ideal of R, an ideal T which is maximal with respect to the requirement that $\bigcap_{g\in G} {}^gT = I$ will be called a *satellite* of I.

Define a *G-variant* ideal of R to be an ideal which is the satellite of some G-invariant ideal. These turn out to be, in some sense, dual to invariant ideals.

For the most part, we will be concerned with prime ideals. Recall that a G-invariant ideal I of R is said to be *G-prime* provided that I does not contain the product of two invariant ideals, each of which properly contains I (see [**9**, p. 342]).

LEMMA 1. (a) *If P is a prime ideal of R then its orb is G-prime.*
(b) *If I is a G-prime ideal of R then its satellites are prime.*

PROOF. (a) This is immediate from the definition of G-prime ideal.

(b) Notice that since R is a noetherian ring, we can certainly produce a satellite P of I. Suppose A and B are ideals containing P such that $AB \subseteq P$.

$$\left(\bigcap_{g\in G} {}^gA\right)\left(\bigcap_{g\in G} {}^gB\right) \subseteq \bigcap_{g\in G} {}^g(AB) \subseteq I$$

Since I is G-prime, we may assume, e.g., that $\bigcap_{g\in G} {}^gA \subseteq I$. But $\bigcap_{g\in G} {}^gP = I$, so $\bigcap_{g\in G} {}^gA = I$. It follows from the maximal property for satellites that $A = P$. □

By using the lemma, it is easy to construct G-prime ideals which are not prime. On the other hand, such ideals are clearly semiprime. Consequently, if I is a G-prime ideal of R then it is a finite intersection

$$I = I_1 \cap I_2 \cap \cdots \cap I_t$$

of prime ideals minimal over I. Moreover, G transitively permutes these primes. We shall call each I_j a *G-component* of I. The point is that the stabilizer of a component has finite index in G, so that we may reduce from G-prime ideals to H-invariant prime ideals if we can handle problems of descending by finite index to a subgroup H in the entire automorphism group.

LEMMA 2. *Suppose P is a prime ideal of R and K is a subgroup of finite index in G. Then every K-component of the K-orb of P is a G-component of the G-orb of P.*

PROOF. Let $t(1), \ldots, t(n)$ be coset representatives for K in G. If $J_1, \ldots, J_s$ are the K-components for $\bigcap_K {}^kP$ then

$$\bigcap_G {}^gP = \bigcap_{i=1}^{s} \bigcap_{j=1}^{n} {}^{t(j)}J_i.$$

Each ${}^{t(j)}J_i$ is a G-conjugate of J_1, which realizes the G-orb of P as a finite intersection of G-conjugates of J_1. A simple primality argument now shows that J_1 is a G-component of the G-orb of P. □

To illustrate the lemma, suppose I is the G-orb of a prime ideal P. Then P lies over some component I' of I. If $H = \mathrm{Stab}_G(I')$ then obviously $I' \subseteq \bigcap_{h\in H} {}^hP$. By the lemma, the H-components of $\bigcap_H {}^hP$ are G-components of I. Hence $\bigcap_{h\in H} {}^hP = I'$. As an immediate consequence, every G-satellite of I is an H-satellite of some (prime!) G-component of I for the appropriate subgroup H of finite index in G.

We tuck away the next lemma for later use.

LEMMA 3. *R satisfies the descending chain condition on G-prime ideals.*

PROOF. Suppose $I \supseteq J$ are two G-prime ideals. If $I_1, \ldots, I_m$ are the components of I and $J_1, \ldots, J_n$ are the components of J then for every d we have $J_1 \cap \cdots \cap J_n \subseteq I_d$, whence $I_d \supseteq J_e$ for some e. Moreover, if $I_d = J_e$ then the orbit of components for I coincides with the orbit of components for J. In this case, $I = J$.

We conclude that a strictly descending chain of G-prime ideals induces a strictly descending chain of components. But R has the descending chain condition on prime ideals. □

2. Invariant variant ideals. The problem considered in this section arose as part of a strategy for generalizing from group rings some theorems about the generators of prime ideals. To wit, given a G-invariant prime ideal Q in R it would be very desirable to know whether Q is generated by invariant elements. Surprisingly, the Brewster-Roseblade Theorem says that for "multiplicative actions" this can virtually be achieved: Q can be generated by linear combinations of units each of which has a finite orbit modulo Q. (We will provide more details in §4.) Thus in this case $Q = (Q \cap S)R$ where S is an affine subalgebra of R invariant under G and G acts like a finite group on $S/Q \cap S$. The effective finiteness of G on the factor ring implies that $Q \cap S$ is G-variant as well. The gist of the major theorem in this section is a converse. The coincidence of invariance and variance forces the induced action to be finite.

THEOREM 4. *Let P be a prime ideal of R which is both G-invariant and G-variant. Then G induces a finite group of automorphisms on R/P.*

We are going to prove an equivalent formulation of the theorem. As an initial reduction we may as well assume that $P = 0$. Thus R is a domain and 0 is G-variant.

The next general assertion is undoubtedly well known.

PROPOSITION 5. *Let R be a commutative noetherian domain. Then any intersection of infinitely many distinct principal ideals is zero.*

PROOF. Denote by S the integral closure of R. It is well known that S is a Krull domain [**5**]. We first argue that each nonzero x in S has only finitely many factorizations, up to order and associates. Without loss of generality x is not a unit. Then it lies in only finitely many height one primes. Equivalently, there is a finite list of height one primes $P(1), \ldots, P(n)$ such that x is a unit in S_P for $P \neq P(j)$. In addition, $S_{P(j)}$ is a DVR, whence a unique factorization domain. Hence x has only finitely many factorizations in $S_{P(j)}$ for $j = 1, \ldots, n$. The claim now follows from the observation that if s and t in S are associates in each S_P as P ranges over the height one primes of S then s and t are associates in S. Indeed, if $st^{-1} = z \in \bigcap S_P$ and $z^{-1} \in \bigcap S_p$ then both z and z^{-1} lie in S.

We need to know that R inherits the finite factorization property. This is immediate if associates in S which lie in R are associates in R. We prove this by showing that nonunits in R remain nonunits in the integral extension S. For suppose $a \in R$ with $a^{-1} \in S$. There exist $r_0, \ldots, r_{d-1} \in R$ with

$$a^{-d} + r_{d-1}a^{-d+1} + \cdots + r_0 = 0 \qquad (d > 0).$$

Hence

$$a^{-1} + r_{d-1} + r_{d-2}a + \cdots + r_0 a^{d-1} = 0$$

which, in turn, implies $a^{-1} \in R$.

Finally, if a nonzero element of R lies in the intersection of infinitely many different principal ideals, it has infinitely many factors no two of which are associate. □

We revert to the standing assumptions.

COROLLARY 6. *Let R be an affine domain. Then 0 is a G-variant ideal if and only if every ideal of R has a finite orbit.*

PROOF. Assume that 0 is G-variant. According to Proposition 5 and the definition of G-variance, every principal ideal in R has a finite orbit. The corollary then follows because every ideal of R is finitely generated.

Conversely, if every ideal has a finite orbit then 0 is the intersection of the finitely many conjugates of any one of its satellites. Since 0 is a prime ideal, it must be its own satellite. □

We have proved, so far, that Theorem 4 is equivalent to

THEOREM 7. *Let R be an affine domain. Then every ideal of R has a finite orbit if and only if G is finite.*

One direction of the theorem is a triviality. The proof of the other is quite involved. However, there is an elementary counting argument that proves Theorem 7 when the coefficient field k is uncountable and G is finitely generated. Suppose this is the case. We argue by induction on the Krull dimension of R. If the dimension is 0 then R is a finite field extension of k; G must be a finite group from Galois theory. If R is not a field then R contains uncountably many maximal ideals. (This is obvious for polynomial rings. For general affine domains, use Noether normalization and the standard comparison theorems for primes in integral extensions.) As a consequence of the Principal Ideal Theorem and the finite generation of ideals, each maximal ideal is the sum of finitely many height one prime ideals. Therefore R has uncountably many height one primes. One the other hand, since G is finitely generated, it has only finitely many subgroups of a given finite index: it has only countably many subgroups of finite index. Using the induction hypothesis and the pigeon-hole principle we see that there must be a subgroup H of finite index in G such that H stablizes each member of an infinite family $\{P_\alpha | \alpha \in \Gamma\}$ of height one prime ideals and H acts like the identity group on R/P_α for each α. Hence if $r \in R$ then ${}^h r - r \in \bigcap_{\alpha\in\Gamma} P_\alpha$ for each $h \in H$. But a second application of the Principal Ideal Theorem implies that the intersection of infinitely many height one prime ideals is zero. Thus $H = 1$.

Any argument along these lines is bound to fail when k is finite. To prove Theorem 7 without restriction, we will need a series of reductions. For the remainder of this section we will assume that *every ideal in R has a finite orbit.* Let K denote the field of fractions of R. If K^* denotes the group of nonzero elements of K and $U(R)$ denotes the group of units of R then our running hypothesis can be restated as follows: every element of $K^*/U(R)$ has a finite orbit.

It is clear that R has a finite set of k-algebra generators which is stabilized by G up to units. There is no harm in localizing at this set thereby assuring that R is generated as an algebra by $U(R)$.

LEMMA 8. *If $R = k[A]$, the group algebra of a finitely generated torsion free abelian group, then G is finite.*

PROOF. Suppose $a \neq 1$ is in A. Then there is a subgroup H with finite index in G such that for each $h \in H$ there is a $u \in k^* \times A$ such that ${}^h(a-1) = u(a-1)$. Now ${}^h a - 1 = ua - u$ implies either

$$u = 1 \quad \text{and} \quad {}^h a = a, \quad \text{or}$$

$$u = -{}^h a \quad \text{and} \quad ua = -1.$$

In the second case $a^{-1} =^h a$. Therefore, by replacing H with a subgroup of index 2 we may assume that each element of H fixes a.

Find such a subgroup for each of the finitely many free generators in some basis for A. Their intersection has finite index in G and must be the identity element. □

LEMMA 9. *We may assume that every element of K with a finite orbit lies in k.*

PROOF. Let L be the subfield of K consisting of elements with a finite orbit. Then L is a finitely generated field extension of k. If H is the simultaneous stabilizer of a finite generating set then $|G : H| < \infty$ and H fixes each element of L. Thus we may replace R with $L \cdot R$ and G with H. Since the field of fractions of $L \cdot R$ remains K, the running hypothesis is maintained. □

As a consequence of this lemma, k is algebraically closed in K. (Every G-conjugate of an algebraic element is an algebraic conjugate.)

The next result is a general Galois-theoretic proposition. Assume that A is an abelian group written multiplicatively and that G is a group acting as automorphisms on A. If $B \supseteq C$ are G-invariant subgroups of A write

$$(B : C)^G = \{b \in B | ({}^g b)b^{-1} \in C \text{ for all } g \in G\}.$$

LEMMA 10. *Let $F|k$ be a field extension and suppose that H is a group of k-automorphisms of F such that $F^H = k$. Then distinct elements of $(F^* : k^*)^H/k^*$ lift to k-linearly independent elements of F.*

PROOF. Suppose not. Choose $x_1, \ldots, x_n$ in $(F^* : k^*)^H$ with n minimal subject to $x_1, \ldots, x_n$ being linearly dependent and having distinct images modulo k^*. Clearly $n > 1$ and we may assume that $x_1 = 1$.

Say $\sum \alpha_i x_i = 0$ with $\alpha_i \in k^*$. Then $\sum \alpha_i ({}^h x_i) = 0$ for all $h \in H$. But ${}^h x_1 = 1$ and ${}^h x_i = \lambda_i(h) x_i$ for some $\lambda_i(h) \in k^*$ whenever $i > 1$. Subtracting, we obtain a shorter dependence for each $h \in H$.

$$\sum_{i>1} \alpha_i (1 - \lambda_i(h)) x_i = 0.$$

Hence $\lambda_i(h) = 1$ for all $h \in H$. That is, ${}^h x_i = x_i$ for each h. Consequently $x_1 \in k$. This contradicts $x_1 \equiv x_i \pmod{k^*}$ unless $i = 1$. We are left with $n = 1$. □

The next lemma is based on a suggestion of P. Linnell. My original proof invoked the Brewster-Roseblade Intersection Theorem instead.

LEMMA 11. *We may assume that G is periodic.*

PROOF. If H is a subgroup of G then the sequence of abelian groups below is exact:

$$(K^* : k^*)^H/k^* \to (K^* : U(R))^H/k^* \to \operatorname{Der}(H, U(R)/k^*).$$

Here the second map is induced from the homomorphism sending $x \in (K^* : U(R))^H$ to ∂_x where $\partial_x(h) \equiv ({}^h x)x^{-1} \pmod{k^*}$. We will be able to speak about the ranks of these abelian groups because $U(R)/k^*$ is finitely generated for affine domains R (see [6]).

For the rest of the lemma we analyze the case that G is infinite cyclic and that H is a subgroup of finite index in G. Since H is also infinite cyclic

$$\operatorname{rk} \operatorname{Der}(H, U(R)/k^*) \leq \operatorname{rk} U(R)/k^*.$$

By Lemma 10,

$$\operatorname{rk}(K^* : k^*)^H/k^* \leq \operatorname{tr.deg.}_k K.$$

Hence the rank of $(K^* : U(R))^H/k^*$ is bounded by an integer independent of H. Now the running hypothesis can be interpreted as saying that

$$K^* = \bigcup_H (K^* : U(R))^H.$$

It follows that the rank of K^*/k^* is finite. This immediately implies that K is algebraic over k. We are done by Galois theory. □

LEMMA 12. *G is finite.*

PROOF. As we mentioned before, $U(R)/k^*$ is a finitely generated abelian group. It is a free abelian group by Lemma 9. According to Lemma 11, the image of G in $\mathrm{Aut}(U(R)/k^*)$ is finite. (This follows from the theorem that $GL(n, \mathbb{Z})$ has a torsion free subgroup of finite index [**14**].) Thus we may assume that

$$U(R) = (U(R) : k^*)^G.$$

Since $U(R)/k^*$ is free we write $U(R) = k^* \times A$ where A is a finitely generated free abelian subgroup of $(K^* : k^*)^G$. It is now a consequence of Lemma 10 that members of A are linearly independent over k. But R is generated by its units. Thus $R = k[A]$; apply Lemma 8. □

3. A dimension equality. Our starting point is the ergodic theorem for group algebras in its general form.

THEOREM ([**12**], POSED IN [**4**]). *Let F be a field which is not an algebraic extension of a finite field. Assume that A is a finitely generated free abelian group and that G is a subgroup of* $\mathrm{Aut}(A)$; *then extend G to a group of F-automorphisms of the group algebra $F[A]$. There exists a maximal ideal $\mathcal{M}$ of $F[A]$ such that $\bigcap_{g\in G} {}^g\mathcal{M} = 0$ if and only if the fixed ring $(F[A])^G$ is F.*

A maximal ideal is the quintessential G-variant ideal. In the theorem, $\mathcal{M}$ is a satellite of 0. The conclusion establishes a correlation between the small sizes of $F[A]/\mathcal{M}$ and the fixed ring. We will see that this phenomenon generalizes.

The hypotheses on the field F is necessary. For a finite field F, every maximal ideal of $F[A]$ has finite orbit (cf. [**3**]). Thus if A is nontrivial, no maximal ideal can ever have orb 0. In this section we frequently make an even tighter restriction on the coefficient field: it will be uncountable. For rational actions, the argument in [**7**] seems to require only that k have characteristic zero. Our use of the uncountability hypothesis is similar to that found in [**10**].

Once again R is an affine k-algebra and G is a group of k-automorphisms of R. We will be comparing a G-variant prime P with its orb I. Following the discussion in §2, there is not loss in assuming that I is a prime ideal. By the dimension $d(P)$, of P, we mean the Krull dimension of R/P.

LEMMA 13. *If P is a G-variant prime ideal with prime orb I then*

$$\mathrm{tr.deg.}_k\, Q(R/I)^G \leq d(P).$$

PROOF. We may assume that $I = 0$. Suppose $x \in Q(R)^G$ and write $x = r/s$. Since $\bigcap_G {}^gP = 0$ there exists an $h \in G$ with ${}^hs \notin P$. By assumption $x = {}^hx$, allowing us to rewrite x as a fraction and assume that $s \notin P$. Now for all $g \in G$

$$({}^gr)s = r({}^gs).$$

If it happens that $r \in P$ then $({}^g r)s \in P$. By primality ${}^g r \in P$ for all $g \in G$. Hence $r = 0$.

We have proved that every nonzero element of $Q(R)^G$ has the form r/s with neither r nor s in P. Thus there is an imbedding $Q(R)^G \to Q(R/P)$. The lemma follows because $d(P) = \text{tr.deg.}_k Q(R/P)$. □

The goal is to prove equality over large fields. We first handle the special case that $I = 0$ and $Q(R)^G = k$, the content of Lemma 17.

LEMMA 14. *If B is an ideal of R then there is a subfield K of k which is finitely generated over its prime field and an affine K-subalgebra S in R such that*

$$R/B = k \otimes_K (S/B \cap S)$$

and S spans R as a vector space over k.

PROOF. This is an application of the fact that affine algebras are noetherian. Choose a finite set of algebra generators ρ for R and a finite set of ideal generators β for B. Write each $x \in \beta$ as $x = \sum f_i(x) a_i$ where $f_i(x) \in k$ and a_i is in the multiplicative monoid generated by ρ. Now let K be the field obtained by adjoining to the prime field all $\lambda_i(x)$ as x ranges over β. Let S be the K-algebra generated by ρ. □

LEMMA 15. *Suppose L is a finitely generated field extension of k. Then L satisfies the countable descending chain condition on subfields over k.*

PROOF. Every subfield containing k is a finitely generated extension of k and has transcendence degree not exceeding $\text{tr.deg.}_k L$. Thus any strictly decreasing uncountable chain of subfields has an uncountable subchain of fields with the same transcendence degree over k. But if $E \supsetneq F$ are in this chain then $[E : F] < \infty$. Thus no member of the chain has an infinite portion of the chain above it; the chain cannot be uncountable. □

LEMMA 16 [**13**]. *Assume R is a k-domain and $Q(R)^G = k$. If K is a subfield of k and S is a K-subalgebra of R such that S spans R as a vector space over k then every nonzero G-invariant ideal of R has nonzero intersection with S.*

PROOF. Let J be a nonzero invariant ideal of R and let w be a shortest nonzero k-linear combination in J, say

$$w = \sum \lambda_i a_i \quad \text{with } \lambda_i \in k, a_i \in S.$$

We may assume $\lambda_1 = 1$. For each $g \in G$ we have ${}^g w \in J$. A shortest length argument now yields

$$({}^g a_1)w - a_1({}^g w) = 0.$$

Equivalently, $a_1^{-1} w \in Q(R)^G$. Thus there is a nonzero element $\lambda \in k$ such that $\lambda a_1 \in J$. Obviously $a_1 \in J \cap S$. □

LEMMA 17. *Assume that k is an uncountable field and that R is a k-domain. If $Q(R)^G = k$ then every satellite of 0 is a maximal ideal.*

PROOF. Let P be a prime ideal of R with $\bigcap_G {}^g P = 0$. Applying Lemma 14, we may assume that K is a subfield of k finitely generated over its prime field, S is an affine K-subalgebra of R which spans R over k, and

$$R/P = k \otimes_K S/S \cap P.$$

Use Lemma 15 to produce a countable subgroup $G(1) \subseteq G$ such that $Q(R)^{G(1)} = k$. Similarly, R is a countable vector space over k and so satisfies the countable descending chain condition on subspaces: there is a countable subgroup $G(2) \subseteq G$ such that $\bigcap_{g \in G(2)} {}^gP = 0$. Thus we may assume G is countable by replacing it with the subgroup generated by $G(1)$ and $G(2)$.

The K-algebra S is a countable set. Since G is countable the G-stable K-algebra T generated by S is countable as well. While T need not be an affine K-algebra we have, at least, $Q(T/T \cap P)$ countable. Also $R/P = k \otimes_K T/T \cap P$ and T spans R over k.

In particular, $\text{tr.deg.}_K Q(T/T \cap P) \leq \aleph_0$ while $\text{tr.deg.}_K k > \aleph_0$. As a consequence, the usual proof of the uniqueness of algebraic closures shows that there is a K-imbedding

$$Q(T/T \cap P) \to \bar{k}$$

into the algebraic closure of k. In conjunction with the tensor product equality, it induces a k-algebra homomorphism

$$R \to R/P \to \bar{k}.$$

Since R is affine and this composite map is the identity on k, its kernel is a maximal ideal $\mathcal{M}$ of R which contains P. Moreover, $\mathcal{M} \cap T = P \cap T$.

Let $J = \bigcap_{g \in G} {}^g\mathcal{M}$. If $J = 0$ the lemma is proved. If not, Lemma 16 implies that $J \cap S \neq 0$. But

$$J \cap S = \bigcap_G {}^g(\mathcal{M} \cap S) = \bigcap_G {}^g(P \cap S) = \left(\bigcap_G {}^gP\right) \cap S = 0. \quad \square$$

Lemma 17 can be regarded as the abstract form of the ergodic theorem we discussed at the beginning of the section. The general dimension equality we are seeking can be obtained from the lemma by replacing the coefficient field k with $Q(R)^G$. Until we get to Theorem 20, assume that R is an affine k-domain and simplify notation by setting $\tilde{k} = Q(R)^G$. If B is any ideal of R write $\tilde{B} = \tilde{k}B$, a $\tilde{k}$-subspace of $Q(R)$. In fact, $\tilde{B}$ is an ideal of $\tilde{R}$. The crucial observations are that

(i) $\tilde{R}$ is an affine $\tilde{k}$-domain,

(ii) G is a group of $\tilde{k}$-automorphisms of $\tilde{R}$, and

(iii) $Q(\tilde{R})^G = Q(R)^G = \tilde{k}$.

LEMMA 18. *Let P be a prime ideal of R such that $\bigcap_G {}^gP = 0$. Then $\tilde{P} \cap R = P$.*

PROOF. Clearly $P \subseteq \tilde{P} \cap R$. If there is not equality, choose $x \in \tilde{P} \cap R$ a shortest $\tilde{k}$-linear combination not in P

$$x = \sum \lambda_i b_i \quad \text{with } \lambda_i \in \tilde{k},\ b_i \in P.$$

Note that if $g \in G$ then ${}^g(b_1)x \in \tilde{P} \cap R$ and $b_1({}^gx) \in P$. By further shortening we obtain

$$({}^gb_1)x - b_1({}^gx) \in P.$$

Hence $({}^gb_1)x \in P$ for all $g \in G$. By hypothesis we can find $h \in G$ with ${}^hb_1 \notin P$. By primality $x \in P$. $\square$

LEMMA 19. *If P is a prime ideal of R such that $\bigcap_G {}^gP = 0$ then $\bigcap_G {}^g(\tilde{P}) = 0$.*

PROOF. Suppose $\bigcap_G {}^gP = 0$ but $\bigcap_G {}^g(\tilde{P}) \neq 0$. If $y \in \bigcap_G {}^g(\tilde{P})$ is nonzero then, as an element of $Q(R)$, it can be written as a fraction. Clearing the denominator, we may assume $y \in R$. In other words, $\bigcap_G {}^g(\tilde{P}) \cap R \neq 0$. However, by Lemma 18

$$\bigcap_G {}^g(\tilde{P}) \cap R = \bigcap_G {}^g(\tilde{P} \cap R) = \bigcap_G {}^gP = 0. \quad \square$$

THEOREM 20. *Assume k is an uncountable field. If P is a G-variant prime ideal of R with prime orb I then*

$$d(P) = \text{tr.deg.}_k Q(R/I)^G.$$

PROOF. We reduce to the case $I = 0$ and adopt the notation set before Lemma 18. Then by Lemma 19, $\bigcap_G {}^g(\tilde{P}) = 0$. We can extend $\tilde{P}$ to a satellite of 0 in $\tilde{R}$. According to Lemma 17, this satellite is a maximal ideal $\mathcal{M}$ of $\tilde{R}$.

$\bigcap_G {}^g\mathcal{M} = 0$ implies $\bigcap_G {}^g(\mathcal{M} \cap R) = 0$. Since P is G-variant and contained in $\mathcal{M} \cap R$ we have $P = \mathcal{M} \cap R$.

Now $\tilde{R}/\mathcal{M}$ is a finite extension of $\tilde{k}$. Hence

$$\text{tr.deg.}_k \tilde{R}/\mathcal{M} = \text{tr.deg.}_k \tilde{k}.$$

Since R/P imbeds in $\tilde{R}/\mathcal{M}$ we obtain

$$d(P) = \text{tr.deg.}_k R/P \leq \text{tr.deg.}_k \tilde{R}/\mathcal{M} = \text{tr.deg.}_k Q(R)^G.$$

The opposite inequality was established earlier, in Lemma 13. $\square$

As an application of the theorem, we can identify a common property of G-variant prime ideals with the same orb. In the best of all possible worlds, two G-invariant prime with orb 0 would be conjugate. This turns out to be true when the action is rational and for prime ideals which are maximal [7]. However, this is not the case for "multiplicative" actions. The ergodic theorem for group algebras is proved by showing that if $F[A]^G = 1$ then every maximal ideal $\mathcal{M}$ for which A survives modulo $\mathcal{M}$ has orb 0. If $F = \mathbb{C}$ and A is the free abelian group on x and y then A survives faithfully modulo $(x - 2, y - 3)$ and modulo $(x - 5, y - \pi)$ but these two ideals cannot be conjugate under the action of $GL(2, \mathbb{Z})$. We do obtain a modest result.

COROLLARY 21. *Assume k is an uncountable field. Two G-variant prime ideals of R with the same orb have the same dimension.*

PROOF. Suppose P and Q are G-variant primes with orb I. If P and Q lie over the same component of I then $d(P) = d(Q)$ by Theorem 20. If not, since the components of I are G-conjugate, we can find a conjugate ${}^gQ$ over the same component as P. Clearly $d(Q) = d({}^gQ)$. $\square$

4. Questions and speculation. We have not analyzed the collection of all G-variant prime ideals in an affine algebra R. For instance, we might consider chains of variant primes and denote by $d^{\text{var}}(P)$ the maximum length of a tower of G-variant prime ideals lying over the G-variant prime P. It turns out that d and d^{var} coincide.

LEMMA 22. *Assume that P is a G-variant prime ideal of R and let $\mathcal{H}$ denote the collection of all G-prime invariant ideals with a satellite which strictly contains P. If Q is a prime ideal above P whose orb is minimal in $\mathcal{H}$ then Q is a minimal prime over P.*

PROOF. Suppose that T is an intermediate prime minimal over P, so $P \subsetneq T \subsetneq Q$. Clearly $\bigcap_G {}^gT \in \mathcal{H}$. Since P is G-variant and $\bigcap_G {}^gQ$ is minimal in $\mathcal{H}$, we have $\bigcap_G {}^gQ = \bigcap_G {}^gT$. According to Theorem 144 of [**5**], the collection $\mathcal{T}$ of all such intermediate primes is infinite; by the Principal Ideal Theorem $\bigcap_{T\in\mathcal{T}} T = P$. Hence

$$\bigcap_G {}^gQ = \bigcap_{T\in\mathcal{T}} \bigcap_G {}^gT = \bigcap_{g\in G} \bigcap_{\mathcal{T}} {}^gT = \bigcap_G {}^gP.$$

This contradicts the assumption that P is G-variant. □

THEOREM 23. *If P is a G-variant prime ideal of R then*

$$d(P) = d^{\mathrm{var}}(P).$$

PROOF. We refer to the previous lemma. If P is a G-variant prime ideal which is not already maximal then the collection $\mathcal{H}$ has minimal members by Lemma 3. Choose Q lying over P according to the lemma. There is no loss of generality in assuming that Q is G-variant without changing the minimal orb. By the conclusion of the lemma, $d(Q) = d(P) - 1$. The theorem follows by induction. □

One could well ask whether all maximal towers of variant primes over P have the same length, $d(P)$. In fact, we do not know of any counterexamples to the following assertion: any prime ideal of R which contains a G-variant prime is itself G-variant.

The proof of the previous theorem also suggests a relation on invariant ideals. If I and J are G-prime invariant ideals define $I\alpha J$ when there exist satellites P of I and Q of J such that $P \subseteq Q$. It is obvious that α is reflexive. Since $I\alpha J$ implies that $I \subseteq J$, it follows that α is antisymmetric. We do not know whether α is transitive. It is conceivable that a better result is true: if $I\alpha J$ and P' is any satellite of I then there exists a satellite Q' of J such that $P' \subseteq Q'$. If so, the equidimensionality statement of Corollary 21 would follow from Lemma 22 without coefficient field restrictions. Indeed, if P is a G-variant prime then $d(P) = d^{\mathrm{var}}(P)$ would coincide with the length of any maximal α-tower of G-prime invariant ideals over the orb of P.

It is not at all clear that §3 requires such enormous fields. Based on Roseblade's work [**12**], we ought to focus on nonabsolute fields (i.e., fields which are not algebraic extensions of finite fields). Unfortunately, we have been unable to prove Theorem 20, even for group algebras, under a more relaxed field hypothesis. This stems from our failure to prove a fidelity conjecture about units on curves over nonabsolute fields.

Let us say that a field k is *rich in units* provided that for every affine k-domain R with Krull dimension one and for every finitely generated group of units U in R there exists a maximal ideal $\mathcal{M}$ of R such that the map from U to its image modulo $\mathcal{M}$ is faithful. Then k is *sufficiently large* when all of its field extensions are rich in units. It is not difficult to see that k is rich in units when it is uncountable. The point is that R has uncountably many maximal ideals. If $x \neq 1$ lies in U and is not

invertible then, since R has Krull dimension one, the ideal $(x-1)$ is contained in only finitely many maximal ideals. Since U is countable, there must be uncountably many maximal ideals $\mathcal{M}$ such that $y-1 \notin \mathcal{M}$ for each $y \neq 1$ in U.

PROPOSITION 24. *Assume that k is sufficiently large. If R is an affine k-domain and V is a finitely generated group of units of R then there exists a maximal ideal $\mathcal{M}$ of R such that the image of V in $R/\mathcal{M}$ is faithful.*

PROOF. First notice that we may replace R with any affine k-algebra between R and $Q(R)$. This "birationality" property allows us to invert finitely many elements in R and thereby assume that V spans R as a vector space over k.

We argue by induction on Krull dimension. If the Krull dimension of R is zero then R is a finite field extension of k. Choose $\mathcal{M}=0$. The proposition is true by definition when R has Krull dimension one. Thus we may assume, using induction and the first paragraph, that V contains an element x transcendental over k and that $k(x)\cdot R$ is not a field. Set $L=k(x)$ and consider LR as an affine L-algebra. By induction there exists a maximal ideal $\mathcal{N}$ of LR such that the image of V in $LR/\mathcal{N}$ remains faithful. Certainly V is preserved in $R/\mathcal{N}\cap R$. Now $\mathcal{N}\cap R$ is a *nonzero* prime ideal of R since $\mathcal{N}\neq 0$. (Clear denominators to descend from $\mathcal{N}$ to $\mathcal{N}\cap R$.) Apply induction once again. □

We digress briefly to review the Brewster-Roseblade Theorem. Let k be a field and let A denote a finitely generated abelian group. If I is an ideal of the group algebra $k[A]$ then $I^\dagger = \{a\in A | a-1\in I\}$. In case $I^\dagger=\{1\}$ we say that I is faithful. Next suppose G acts like a group of automorphisms of A. Set $\Delta=\{a\in A | a$ has a finite G-orbit$\}$, a G-invariant subgroup of A. Finally, extend G to a group of algebra automorphisms of $k[A]$. One formulation of the fundamental theorem [**12**] states that if I is a faithful G-invariant prime ideal of $k[A]$ then $I=(I\cap k[\Delta])k[A]$.

THEOREM 25. *Assume k is a sufficiently large field and let I be a G-invariant faithful prime ideal of $k[A]$. If P is a satellite of I then*

$$d_{k[A]}(P) = d_{k[\Delta]}(I\cap k[\Delta]).$$

PROOF. Without loss of generality Δ consists of those elements of A fixed by G. As a consequence of Proposition 24, we can find a maximal ideal $\mathcal{M}\supseteq P$ with $P^\dagger = \mathcal{M}^\dagger$. A slight variation of Lemma 22 allows us to construct a chain of prime ideals

$$P_0 \underset{\neq}{\subset} P_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} P_n$$

where $P_0=P$, $P_n=\mathcal{M}$, each P_i is G-variant, and $d(P_{i+1})=d(P_i)-1$. Let I_j denote the component of the orb of P_j which is contained in P_j. By dropping to a subgroup of finite index we may assume that I_j is actually the orb of P_j for $j=1,\ldots,n$.

We claim that each I_j is faithful. Indeed, $I=\bigcap_G {}^gP$ (even after the replacement of G with a subgroup of finite index). Hence

$$\{1\} = I^\dagger = \bigcap_G {}^g(P^\dagger).$$

But $P_j^\dagger = P^\dagger$. Therefore

$$I_j^\dagger = \bigcap_G {}^g(P_j^\dagger) = I^\dagger = \{1\}.$$

Next, notice that

$$I_j \cap k[\Delta] = \bigcap_G {}^g(P_j \cap k[\Delta]) = P_j \cap k[\Delta].$$

The Brewster-Roseblade Theorem then yields

$$I_j = (P_j \cap k[\Delta])k[A].$$

The G-variance of each P_j implies that no two I_j are equal. Hence we have a strictly increasing chain

$$P_0 \cap k[\Delta] \subsetneq P_1 \cap k[\Delta] \subsetneq \cdots \subsetneq P_n \cap k[\Delta].$$

Therefore $d(I \cap k[\Delta]) \geq d(P)$.

On the other hand, $k[\Delta]/I \cap k[\Delta]$ injects in $k[A]/P$. Comparing transcendence degrees we see that $d(I \cap k[\Delta]) \leq d(P)$. □

Theorem 20 can be recovered for group algebras with well-known techniques developed by M. Smith and Roseblade. See §2 of [**1**] for details.

REFERENCES

1. D. R. Farkas, *Multiplicative invariants*, Enseign. Math. **30** (1984), 141–157.
2. ____, *Recurrent behavior in rings*, J. Algebra **108** (1987), 127–138.
3. ____, *Toward multiplicative invariant theory*, Contemp. Math., vol. 43, Amer. Math. Soc., Providence, R. I., 1985, pp. 69–80.
4. D. R. Farkas and D. S. Passman, *Primitive noetherian group rings*, Comm. Algebra **6** (1978), 310–315.
5. I. Kaplansky, *Commutative rings*, Allyn and Bacon, Boston, Mass., 1970.
6. S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, Berlin, 1983.
7. C. Moeglin and R. Rentschler, *Orbites d'un groupe algébrique dans l'espace des idéaux rationnels d'une algèbre enveloppante*, Bull. Soc. Math. France **109** (1981), 403–426.
8. M. Nagata, *Lecture notes on the fourteenth problem of Hilbert*, Lecture Notes in Math., Vol. 31, Tata Institute, 1964.
9. D. S. Passman, *The algebraic structure of group rings*, Wiley-Interscience, New York, 1977.
10. ____, *Primitive group rings*, Pacific J. Math. **47** (1973), 499–506.
11. R. Rentschler, *Primitive ideals in enveloping algebras (general case)*, Noetherian Rings and Their Applications, Math. Surveys and Monos., no. 24, Amer. Math. Soc., Providence, R. I., 1987.
12. J. E. Roseblade, *Prime ideals in group rings of polycyclic groups*, Proc. London Math. Soc. (3) **36** (1978), 385–447.
13. M. K. Smith, *Group algebras*, J. Algebra **18** (1971), 477–499.
14. B. A. F. Wehrfritz, *Infinite linear groups*, Springer-Verlag, New York, 1973.

DEPARTMENT OF MATHEMATICS, VIRGINIA POLYTECHNIC INSTITUTE & STATE UNIVERSITY, BLACKSBURG, VIRGINIA 24061