Augmentation modules for affine groups

Christopher J. B. Brookes

Corpus Christi College, Cambridge CB2 1RH

email: brookes@dpmms.cam.ac.uk

and

David M. Evans

School of Mathematics, University of East Anglia, Norwich NR4 7TJ

email: d.evans@uea.ac.uk

ABSTRACT: We prove that if k, F are fields of different characteristics then the permutation module kF^n for the affine group $AGL(n, F)$ has simple augmentation submodule. This proves a conjecture of A. R. Camina.

1. *Introduction*

Suppose k and F are (commutative) fields of characteristics l and p respectively. Write A for the additive group of the n-dimensional vector space F^n and Q for its automorphism group, and consider the affine group $G = A.Q$ acting on F^n (as $x \mapsto qx + a$ for $x \in F^n$, $q \in Q$ and $a \in A$). We are interested in the submodule structure of the kG-permutation module kF^n. Equivalently, consider the group algebra kA with Q acting on it (via conjugation in G). Then the kG-submodules of kF^n are exactly the Q-invariant ideals in kA. We write A multiplicatively from now on, and denote the Q-action on the right as a superscript.

For any group B denote by $I(B)$ the augmentation ideal of the group algebra kB. Thus $I(B)$ is the kernel of the augmentation map $kB \to k$ (with $\sum_{b\in B} \alpha_b b \mapsto \sum_{b\in B} \alpha_b$). Our main result is the following, which proves a conjecture of Alan Camina (personal communication):

Theorem 1 *Let the characteristics of k and F be different. Then the zero ideal is the only Q-invariant ideal of kA strictly contained in $I(A)$. When F is infinite, the Q-invariant ideals of kA are $0, I(A)$ and kA. When F is finite, there is an additional Q-invariant ideal, that generated by $\sum_{a\in A} a$.*

Expressed in terms of permutation modules, this says that the augmentation submodule of the kG-permutation module kF is simple when the characteristics of F and k are different. Special cases of this result were known previously. The case $n = 1$ is handled when $F = \mathbb{Q}$ by A. R. Camina and D.M. Evans in [2] and when F is a finite extension of $\mathbb{Q}$ by D. R. Farkas and R. L. Snider in [3]. If F is finite the result is 'well-known' and the locally finite case follows easily from this. Note that, as any element of kA is contained in kA_1 where A_1 is the additive group of F_1^n for some countable subfield F_1 of F, it is enough to prove Theorem 1 in the case where F is countable.

The proof of Theorem 1 varies according to whether the characteristic of F is zero or not, but the strategy of the proof is the same in all cases. Let Q_0 denote the multiplicative group of the prime subfield F_0 of F. So we may consider A as an F_0-vector space. We consider semiprime ideals of kA which are contained in $I(A)$ and which are Q_0-invariant (recall that an ideal J in a commutative ring R is *semiprime* if R/J has no non-zero nilpotent elements). Suppose B is a subgroup of A. The natural homomorphism $A \to A/B$ induces a k-algebra homomorphism $kA \to k(A/B)$ whose kernel consists of all $\sum_{x\in A} \alpha_x x$ with the property that $\sum_{x\in T} \alpha_x = 0$ for all cosets T of B in A. It is easy to see that this equals $I(B)kA$.

Proposition 2 *Assume either that F is of characteristic zero, or that the characteristics of k and F are different. Suppose $J < I(A)$ is a Q_0-invariant semiprime ideal. Then there exists a proper F_0-subspace B of A such that $J \leq I(B)kA$.*

This is proved in Section 2. Most work is needed when the characteristic of F is zero and valuation-theoretic techniques come into play. The other main ingredient in the proof of Theorem 1 is Proposition 3, which we prove in Section 3.

Proposition 3 *Suppose either that F is of characteristic 0, or of different characteristic to k. Let B be a proper F_0-subspace of A. Then*

$$\bigcap_{q\in Q} I(B^q)kA = \{0\}.$$

Proof of Theorem 1: Let I be a non-zero Q-invariant ideal in kA. If its intersection with $I(A)$ is zero then it is one dimensional as a k-vector space and A acts trivially upon it. This can only happen when A is finite and I is the ideal generated by $\sum_{a\in A} a$. So suppose $I \cap I(A)$ is non-zero. We shall show that this implies that $I(A) \leq I$. It follows that I is $I(A)$ or kA as required. So it is enough to consider the case where $I \leq I(A)$.

Let J be the radical of I (that is, the smallest semiprime ideal of kA containing I). Then $J \leq I(A)$ is a Q-invariant semiprime ideal of kA. It follows from Propositions 2 and 3 that $J = I(A)$.

Let $u = a - 1 \in I(A)$ (for some $a \in A \setminus \{1\}$). Then there exists a natural number m such that $u^m \in I$. Choose m as small as possible. It is enough to prove that $m = 1$.

Case $l \neq 0$. Let s be the non-negative integer such that $l(s-1) < m \leq ls$. Then $(a^l - 1)^s = (a-1)^{ls} \in I$, and so $(a-1)^s \in I$, by Q-invariance. Hence, $s \geq m$. If $s = 1$, we are done. If $s > 1$ then $\frac{s}{s-1} > l$, which contradicts $l \geq 2$.

Case $l = 0$. In the polynomial algebra $k[X]$, the greatest common divisor of $(X-1)^m$ and $(X^p - 1)$ is $X - 1$. Since $a^p = 1$ we see that $(a-1)^m \in I$ forces $a - 1 \in I$. □

The Propositions 2 and 3 also give information when the characteristics of k and F are both zero. We are grateful to J.E. Roseblade for providing us with the following argument, depending crucially on certain binomial coefficients being non-zero in k; the strategy is similar to that of the proof of the Nagata-Higman theorem to be found on p.274 of [4]. On the other hand, when the characteristics are both equal to $p > 0$ we do not know whether all non-zero Q-invariant ideals of kA necessarily contain a positive power of $I(A)$.

Theorem 4 *Suppose k and F are of characteristic zero. Then any non-zero Q-invariant ideal of kA contains a positive power of the augmentation ideal $I(A)$ of A.*

Proof. Let J be the radical of a non-zero, proper, Q-invariant ideal I. By Propositions 2 and 3 we again know that J is $I(A)$, and so $(a-1)^m$ lies in I for some m and some non-identity $a \in A$. Since Q acts transitively and I is invariant this implies $(a-1)^m \in I$ for all $a \in A$.

Let I_r be the ideal generated by the set of $(a-1)^r$ with $a \in A$. Thus the ideals I_r are Q-invariant and $I_m \leq I$. We prove by induction that $I_r \geq I(A)^{2^{r-1}}$ by showing that $I_{r-1}^2 \leq I_r$ for each r and observing that $I_1 = I(A)$.

First note that $ab - 1 = (a-1)b + (b-1)$. Set $\alpha = (a-1)b$ and $\beta = b - 1$. Thus $(\alpha+\beta)^r \equiv 0 \pmod{I_r}$. We show that $\alpha^{r-1}\beta^{r-1} \equiv 0$.

If r is even, set $r = 2s$ and observe that $\alpha^{s-1}(\alpha+\beta)^r\beta^{s-1} \equiv 0$. Expanding and using that $\alpha^{2s} \equiv 0 \equiv \beta^{2s}$ we find that

$$\alpha^{s-1}\binom{2s}{s}\alpha^s\beta^s\beta^{s-1} \equiv 0.$$

Since the characteristic of k is zero this implies that $\alpha^{r-1}\beta^{r-1} \equiv 0$. Similarly if $r = 2s+1$ the expansion of $\alpha^s(\alpha+\beta)^r\beta^{s-1} \equiv 0$ yields $\alpha^{r-1}\beta^{r-1} \equiv 0$.

Since b is a unit we deduce that $(a-1)^{r-1}(b-1)^{r-1} \in I_r$ for all a and b in A, and therefore that $I_{r-1}^2 \leq I_r$. □

2. Proof of Proposition 2

2.1. The case char $F = 0$.

Lemma 5 *Let $A \leq B$ be finitely generated abelian groups and k be a field. Let J be a semiprime ideal of kB. Denote the primes of kB minimal over J by $P_1, P_2, \ldots, P_m$ and those of kA minimal over $J \cap kA$ by $Q_1, Q_2, \ldots, Q_r$.*

Then for each i there is some j with $P_i \cap kA \geq Q_j$, and each Q_j is of the form $P_i \cap kA$ for some i. Thus each Q_j extends, not necessarily uniquely, to a prime P_i.

Proof. Because $P_i \geq J$ we have $P_i \cap kA \geq J \cap kA$. But $P_i \cap kA$ is prime in kA and so contains some prime Q_j minimal over $J \cap kA$.

A semiprime ideal is the intersection of the primes minimal over it and so the product $P_1 \ldots P_m \leq \bigcap_{i=1}^m P_i = J$. Hence $\prod_i (P_i \cap kA) \leq J \cap kA = \bigcap_j Q_j \leq Q_j$ for each j. But Q_j is prime and so some $P_i \cap kA \leq Q_j$. But $P_i \cap kA$ is prime in kA and so the minimality of Q_j ensures $P_i \cap kA = Q_j$. □

Proposition 6 *Let A be isomorphic to the additive group $\mathbb{Q}^n$ and k be a field. Consider the multiplicative group $\mathbb{Q}^\times$ acting on A, via multiplication, and hence on kA. Let J be a semiprime ideal of kA invariant under this action.*

Then there are finitely many primes of kA minimal over J and they are of the form $I(B_i)kA$ where $I(B_i)$ is the augmentation ideal of the subgroup B_i of A corresponding to a rational subspace of $\mathbb{Q}^n$ (for $i = 1, \dots, m$). Thus $J = \bigcap_{i=1}^m I(B_i)kA$.

Remark. Since each $\mathbb{Q}^\times$-invariant semiprime ideal of kA is the intersection of finitely many primes, of the form $I(B)kA$, the set of $\mathbb{Q}^\times$-invariant semiprime ideals satisfies the maximum condition.

Before starting the proof, we recall a definition. Suppose A is an abelian group (written multiplicatively). We say that an ideal P in its group ring kA is *faithful* if $(P+1) \cap A = \{1\}$. Equivalently, the natural homomorphism embeds A into the group of units of kA/P.

Proof of Proposition 6. We choose finitely generated subgroups A_j with $A_1 < A_2 < \dots$ and $\bigcup_j A_j = A$ so that $A_j = A_1^{q_j}$ for some $q_j \in \mathbb{Q}^\times$. For example within $\mathbb{Q}^n$ we may pick

$$\mathbb{Z}^n < \frac{1}{2}\mathbb{Z}^n < \frac{1}{2^2.3}\mathbb{Z}^n < \frac{1}{2^3.3^2.5}\mathbb{Z}^n < \dots.$$

Since J is semiprime, $J \cap kA_j$ is also semiprime and therefore the intersection of the finitely many primes minimal over it. But $J = J^{q_j}$ and so $J \cap kA_j = (J \cap kA_1)^{q_j}$. Denoting the minimal primes over $J \cap kA_1$ by $Q_1, \dots, Q_m$ the minimal primes over $J \cap kA_j$ are $Q_1^{q_j}, \dots, Q_m^{q_j}$. Thus the number of primes minimal over $J \cap kA_j$ is independent of j. Lemma 5 says that each prime minimal over $J \cap kA_1$ extends to one minimal over $J \cap kA_j$, and, because the numbers of such primes are the same, this extension is unique. Taking the union over j of the extensions of Q_i in kA_j minimal over $J \cap kA_j$ gives a prime P_i of kA with $P_i \cap kA_j$ minimal over $J \cap kA_j$ for all j and $P_i \cap kA_1 = Q_i$. Thus $P_i \geq J$ and, since $(\bigcap_i P_i) \cap kA_j = \bigcap_i (P_i \cap kA_j) = J \cap kA_j$ for all j, we have $\bigcap_i P_i = J$. Also, no P_i contains any other. Indeed the P_i are precisely the primes of kA minimal over J. To see this consider any prime P of kA containing J. Then the product $P_1 \dots P_m \leq \bigcap_i P_i = J \leq P$ and so $P_i \leq P$ for some i using the primality of P.

Now consider the action of $\mathbb{Q}^\times$. If $q \in \mathbb{Q}^\times$ then $P_1^q, \dots, P_m^q$ are the primes minimal over $J^q = J$. Thus $\mathbb{Q}^\times$ permutes the primes P_i. Some subgroup S of finite index in $\mathbb{Q}^\times$ fixes each P_i. Let $B_i = (P_i + 1) \cap A$. For each i this is a subgroup of A invariant under S, and $I(B_i)kA \leq P_i$. The only subgroups of $\mathbb{Q}^n$ invariant under a subgroup of finite index in $\mathbb{Q}^\times$ are the additive groups of vector subspaces and so B_i is such a subspace.

Consider the image of P_i in $k(A/B_i)$. It is faithful and invariant under the inherited action of S on $k(A/B_i)$. In addition, S contains a positive integer which, when k has positive characteristic, may be chosen coprime to the characteristic. Thus the following proposition ensures that the image of P_i in $k(A/B_i)$ is zero. The kernel of the natural map $kA \to kA/B_i$ is $I(B_i)kA$, and so we obtain $P_i = I(B_i)kA$. □

Proposition 7 *Let A be isomorphic to the additive group of a finite dimensional rational vector space (written multiplicatively), and k be a field of characteristic p. Let P be a prime ideal of kA with $(1+P) \cap A = 1$. Let m be a positive integer greater than 1, coprime to p in the case when $p > 0$. Let γ be the ring automorphism of kA induced by the group automorphism of A obtained by taking mth roots. Suppose that P is invariant under γ. Then P is zero.*

Proof. Suppose that P is non-zero. We may assume, by passing to the intersection of P with the group algebra of a subgroup corresponding to a rational subspace, that $P \cap kB = 0$ for any subgroup B of A of smaller torsion-free rank.

For subgroups B of A we shall write $k[B]$ for the integral domain $kB/(P \cap kB)$ and $k(B)$ for its field of fractions. Note that as P is non-zero, the transcendence degree of $k(A)$ over k is less than the torsion free rank of A. The minimality assumption of the previous paragraph ensures that $k(A)$ is algebraic over $k(B)$ whenever the torsion-free rank of A/B is equal to 1. Since $(1+P) \cap A = 1$ there is a natural embedding of A into $k(A)$.

Suppose first that A has torsion-free rank 1. Then kA/P is an algebraic field extension of k. If $a \in A$ is not 1 then $k[< a >]$ is a field extension of finite degree d say. Applying the automorphism γ we discover that $k[< a^{1/m} >]$ is also of degree d over k. But this field contains $k[< a >]$ and so is equal to it. Thus $k[< a >]$ is invariant under the k-automorphism γ. So some non-zero power γ^s of γ fixes $k[< a >]$ and hence $a^{1/m^s} - a \in P$. Hence $a^{1/m^s}a^{-1} \in (1+P) \cap A$, contradicting the faithfulness of P.

Thus the torsion-free rank of A is greater than 1, and so the minimality assumption of the first paragraph together with the above argument, imply that only the trivial element of A yields an image in $k[A]$ algebraic over k. Thus $k(A)$ has transcendence degree at least 1 over k. Let A_0 be a free Abelian subgroup of A of maximal rank. Then $k(A)$ has the same transcendence degree over k as $k(A_0)$ and so $P \cap kA_0$ is non-zero, but $P \cap kB_0 = 0$ for any subgroup B_0 of A_0 of smaller rank. Thus $k(A_0)$ is algebraic over $k(B_0)$ whenever A_0/B_0 is infinite cyclic.

Take $C_0 \leq A_0$ such that the transcendence degree of $k(A_0)$ over $k(C_0)$ is 1 and let $x \in A_0$ be transcendental over $k_1 = k(C_0)$. Let v_1 be the valuation on $k_1(x)$ obtained by localising the polynomial ring $k_1[x]$ at x. This valuation is discrete with x taking value 1 and the characteristics of k and the residue field of the valuation ring are the same. As $k(A_0)$ is finitely generated over k it is a finite extension of $k_1(x)$, and so v_1 extends to a discrete valuation v on $k(A_0)$. Now let B_0 be the intersection of A_0 with the kernel of v. Thus A_0/B_0 is an infinite cyclic group and there is some $a \in A$ with $A_0 = B_0 < a >$.

The discrete valuation v extends to one on the field $k(B_0^{1/m} < a >)$. We need to establish that no ramification takes place. We refer the reader to VI.8.5 of Bourbaki [1] for the standard theory of the behaviour of valuations under field extension. Our field extension is obtained by adjoining mth roots of elements of value 0. It is therefore enough to show that such a valuation v on a field K does not ramify on extending to a valuation w on $L = K(\alpha^{1/m})$ when α has value 0. This is probably well-known, but we include a proof, for lack of a suitable reference. Write $\hat{K}$ and $\hat{L}$ for the completions with respect to v and w. Since L is a separable extension of K, the characteristic being coprime to m, we know that $\hat{K} \otimes L$ is isomorphic to a direct product of fields $\hat{L}_i$, one of which is isomorphic to $\hat{L}$. Moreover, if $f(X)$ is the minimal polynomial of $\alpha^{1/m}$ over K, then $\hat{L}$ is isomorphic to $\hat{K}[X]/(f_i(X))$ where $f_i(X)$ is one of the irreducible factors of $f(X)$ in $\hat{K}[X]$, and the degree of $f_i(X)$ is equal to the product of the ramification index e of w over v with the degree t of the residue field L_w over the residue field K_v. However $f(X)$ divides $X^m - \alpha$ and all its coefficients lie in the valuation ring of v. Since m is coprime to the characteristic of the residue field K_v, we know that $f(X)$ does not have repeated roots modulo the unique maximal ideal $\mathcal{P}$ of the valuation ring of v. Hensel's lemma says that in such circumstances any factorisation of $f(X)$ modulo $\mathcal{P}$ induces a factorisation of $f(X)$ over $\hat{K}$. Thus the irreducibility of $f_i(X)$ in $\hat{K}[X]$ ensures that $f_i(X)$ is irreducible modulo $\mathcal{P}$. However $f_i(X)$ modulo $\mathcal{P}$ does have a root in the residue field L_w, namely a root of $f_i(X)$ in $\hat{L}$ modulo the maximal ideal of the valuation ring, and so the degree of $f_i(X)$ is at most equal to the degree t of the extension L_w over K_v. Thus $et \leq t$ and so $e = 1$.

The value group of the extended valuation on $k(B_0^{1/m} < a >)$ is therefore precisely that of v. Repeated extension in this way yields a discrete valuation w_1 on $k(D < a >)$, where D is the closure of B_0 under taking mth roots. Let d be the degree of the algebraic extension $k(D < a >)$ of $k(D)$. Applying the automorphism γ, we get that $k(D < a^{1/m} >)$ also has degree d over $k(D)$. Since one extension lies in the other they must be the same field and it is closed under the automorphism induced by γ. It is therefore $k(E)$ where E is the closure of A_0 under $< \gamma >$. The valuation w_1 therefore induces a non-trivial group homomorphism from the m-divisible group E to the value group which is infinite cyclic, a contradiction. □

Proposition 8 *Let A be isomorphic to the additive group of a countably infinite dimensional $\mathbb{Q}$-vector space and k be a field. Suppose J is a semiprime ideal of kA invariant under the action of $\mathbb{Q}^\times$.*

Then J is the intersection of some primes of the form $I(B)kA$ where the subgroups B correspond to the additive groups of vector subspaces. In particular J is contained in some $I(B)kA$.

Proof. We may pick subgroups A_j isomorphic to $\mathbb{Q}^j$ so that $A_1 < A_2 < \ldots$ and $\bigcup_j A_j = A$. By Lemma 5, each prime minimal over $J \cap kA_j$ extends to a prime minimal over $J \cap kA_{j+1}$. Taking the union of such a chain of minimal primes gives a prime P of kA containing J, since $P \cap kA_j$ contains $J \cap kA_j$ for each j. But each $P \cap kA_j$ is a minimal prime over $J \cap kA_j$, which is a semiprime ideal of kA_j invariant under the action of $\mathbb{Q}^\times$, and so is of the form $I(B_j)kA_j$ for some additive group B_j of a vector subspace of A_j, by Proposition 6. Thus $B_1 \leq B_2 \leq \ldots$ and setting $B = \bigcup_j B_j$ we have $B \cap A_j = B_j$ and $P = I(B)kA$. Thus $J \leq I(B)kA$. In fact considering the set X of all primes P obtained in this way by extending primes minimal over some $J \cap kA_j$ one can see that

$$J \cap kA_j = \bigcap_{P \in X} (P \cap kA_j) = (\bigcap_{P \in X} P) \cap kA_j$$

for each j and so $J = \bigcap_{P \in X} P$. □

In the case where char $F = 0$, Proposition 2 now follows immediately from Propositions 6 and 8.

2.2. The case char $F \neq 0$.

Lemma 9 *Let p be a prime, $m \in \mathbb{N}$, and $A_m = \langle x_1, \ldots, x_m \rangle$ an elementary abelian group of order p^m. Let Q_0 consist of the automorphisms of A_m given by $a \mapsto a^i$, for $a \in A$ and $1 \leq i \leq p-1$. Let k be a field of characteristic $l \neq p$. Suppose J_m is a semiprime ideal in the group algebra kA_m which is properly contained in $I(A_m)$, and which is Q_0-invariant. Then there is a proper subgroup B_m of A_m such that $J_m \leq I(B_m)kA_m$. In fact, J_m can be written as the intersection of ideals of this form.*

Proof. There is no loss of generality in assuming that k contains a primitive p-th root of unity, ζ. The group ring kA_m is isomorphic to the polynomial ring $k[X_1, \ldots, X_m]$ factored by the ideal I generated by the polynomials $X_i^p - 1$ (for $i = 1, \ldots, m$). Thus the semiprime ideals in kA_m are in one-to-one correspondence with semiprime ideals in $k[X_1, \ldots, X_m]$ which contain I, and by the Nullstellensatz these are precisely the annihilators of subsets of

$$\{(\zeta^{j_1}, \ldots, \zeta^{j_m}) : 0 \leq j_i \leq p-1\}.$$

Denoting the field of integers modulo p by $\mathbb{F}_p$, this implies that there exists a non-zero $\mathbf{j} = (j_1, \ldots, j_m) \in \mathbb{F}_p^m$ such that if $f = \sum_{\mathbf{i} \in \mathbb{F}_p^m} \alpha_{\mathbf{i}} x^{\mathbf{i}}$ is in J_m then $\sum_{\mathbf{i}} \alpha_{\mathbf{i}} \zeta^{\mathbf{i} \cdot \mathbf{j}} = 0$, where $x^{\mathbf{i}} = x^{i_1} \cdots x^{i_m}$ and $\mathbf{i} \cdot \mathbf{j}$ denotes the dot product in $\mathbb{F}_p^m$. For $r \in \mathbb{F}_p$ let $c_r = \sum\{\alpha_{\mathbf{i}} : \mathbf{i} \cdot \mathbf{j} = r\}$. It will be enough to show that each c_r is zero, for then $f \in I(B_m)kA_m$, where $B_m = \{x^{\mathbf{i}} : \mathbf{i} \cdot \mathbf{j} = 0\}$. But invariance of J_m under the action of Q_0 means that for $s = 1, \ldots, p-1$ we have

$$\sum_r c_r \zeta^{rs} = 0.$$

As $J_m \leq I(A)$ we also have

$$\sum_r c_r = 0.$$

Consideration of the Vandermonde matrix with first row $1, \zeta, \ldots, \zeta^{p-1}$, noting that these are all distinct, then shows that each c_r is zero, as required. $\square$

Proof of Proposition 2. We may assume that F is countable. Let $x_1, x_2, \ldots$ be a basis for A a Q_0-space, and let $A_m = \langle x_1, \ldots, x_m \rangle$. Then $J_m = kA_m \cap J$ is a Q_0-invariant semiprime ideal in kA_m, which is properly contained in $I(A_m)$ if m is large enough. In particular, there exists a t such that $x_t - 1 \notin J$. Note that for $B \leq A$ and $a \in A$ we have $a - 1 \in I(B)kA$ if and only if $a \in B$. Thus, by the above lemma, for $m \geq t$ there is $B_m \leq A_m$ with $x_t \notin B_m$ and $J_m \leq I(B_m)kA_m$. Also note that

$$(I(B_{m+1})kA_{m+1}) \cap kA_m = I(B_{m+1} \cap A_m)kA_m.$$

Thus an application of König's lemma shows that there exists $B \leq A$ with $x_t \notin B$ and $J \leq I(B)kA$, as required. $\square$

3. Proof of Proposition 3

The proof splits into two cases, depending on the characteristic of F, but in both cases we require the following 'density' result, which may be of independent interest.

Lemma 10 *Let F be a field with prime subfield F_0, and let $\alpha : F^n \to F_0$ be a non-zero F_0-linear map. For $g \in GL(n,F)$ define α^g by $\alpha^g(x) = \alpha(g(x))$ (where $x \in A$). Let V be a finite dimensional F_0-subspace of F^n and $\alpha_0 : V \to F_0$ be an F_0-linear map, assumed to be non-zero in the case where $V = F^n$. Then there exists $g \in GL(n,F)$ such that for all $x \in V$ we have $\alpha_0(x) = \alpha^g(x)$.*

Proof. Pick an F-basis $e_1, \ldots, e_n$ of F^n so that $\alpha(e_i) \neq 0$ for each i, and let α_i be a non-zero element of the F_0-dual space of a finite dimensional F_0-vector space $W_i \leq Fe_i$. As the multiplicative group Q_1 of F is transitive on $F \setminus \{0\}$, it is clear that $Fe_i \cap \bigcap_{q \in Q_1} ker(\alpha^q) = \{0\}$. Thus $\bigcap_{q \in Q_1} ker(\alpha^q \mid W_i) = \{0\}$ and so (as W_i is finite dimensional) $\{\alpha^q \mid W_i : q \in Q_1\}$ spans the dual space of W_i. Thus there exist $q_1, \ldots, q_r \in Q_1$ and $\mu_1, \ldots, \mu_r \in F_0$ such that for all $x \in W_i$

$$\alpha_i(x) = \sum_{i=1}^{r} \mu_i \alpha^{q_i}(x) = \alpha((\sum_{i=1}^{r} \mu_i q_i)x).$$

Let $\lambda_i = \sum_i \mu_i q_i$ and, noting that λ_i is non-zero, let g_1 be the element of $GL(n,F)$ for which each e_i is a λ_i-eigenvector. Thus α^{g_1} coincides with α_i on W_i for each i.

Now consider the given element α_0 of the F_0-dual space of V. Suppose α_0 is zero. Then by assumption $V \neq F^n$ and we can extend α_0 to give a non-zero element α' in the dual space of a finite dimensional F_0-vector space $V' > V$. If α^g restricts to give α' on V' then on V it coincides with α_0. Thus, by replacing V by V', we may assume α_0 is non-zero.

Now choose an F_0-basis of V with each element taking non-zero value with respect to α_0. Taking a maximal F-linearly independent subset $e'_1, \ldots, e'_s$ of this basis gives a F-basis of FV; extend it to a basis $e'_1, \ldots, e'_n$ of F^n. Let $g_2 \in GL(n,F)$ be such that $g_2(e'_i) = e_i$ for each i. By enlarging V if necessary, we may assume that $V = \bigoplus_{i=1}^n V_i$ with $V_i \leq Fe'_i$. Let $W_i = g_2(V_i)$ and define α_i by $\alpha_i(g_2(x)) = \alpha_0(x)$ for $x \in V_i$. Thus $W_i \leq Fe_i$ and α_i is a non-zero element of the F_0-dual space of $g_2(V_i)$. So there is $g_1 \in GL(n,F)$ such that $\alpha^{g_1}(g_2(x)) = \alpha_i(g_2(x)) = \alpha_0(x)$ for $x \in V_i$. Hence $\alpha^{g_1 g_2}(x) = \alpha_0(x)$ for $x \in V_i$ and so $\alpha^{g_1 g_2}$ and α_0 coincide on $V = \bigoplus_{i=1}^n V_i$. Setting $g = g_1 g_2$ gives the required element of $GL(n,F)$. □

We complete the proof of Proposition 3. First, suppose that the characteristic of F is zero, so $F_0 = \mathbb{Q}$. Let $0 \neq v = \sum_{a \in A} \gamma_a a \in kA$. To prove the proposition it will suffice to assume that the proper F_0-subspace B is of codimension 1 in A and to find $g \in Q$ such that $v \notin I(B^g)kA$.

Let $S = \{a \in A : \gamma_a \neq 0\}$. Recall that $I(B)kA$ is the kernel of the natural map $kA \to k(A/B)$ and so consists of those $\sum_{a \in A} \beta_a a \in kA$ such that $\Sigma_{a \in C} \beta_a = 0$ for every coset $C \in A/B$. Thus it is enough to show that we can find $g \in Q$ such that no two elements of S lie in the same coset of B^g in A. Let $Y = \{a_1 - a_2 : a_1, a_2 \in S, \text{distinct}\}$. Then Y is finite, and it will suffice to find

$g \in Q$ such that $Y \cap B^g = \emptyset$. However B is the kernel of a non-zero element α of the F_0-dual space of A. We therefore want to find $g \in Q$ such that $\alpha^g(y) \neq 0$ for all $y \in Y$. Let V be the F_0-subspace of A generated by Y. As F_0 is infinite, there exists an F_0-linear map $\alpha_0 : V \to F_0$ such that $\alpha_0(y) \neq 0$ for $y \in Y$. An application of Lemma 10 gives the required element of Q.

Finally, suppose the characteristic of F is non-zero, and different from the characteristic of k. Let V be a finite dimensional F_0-subspace of F. As $(I(B)kA) \cap kV = I(B \cap V)kV$ for any subgroup B of A, it follows from Lemma 10 that it is enough to show

$$X = \bigcap \{I(W)kV : W \text{ a hyperplane in } V\} = \{0\}.$$

But X is an F_0-invariant semiprime ideal of kV, and the required result therefore follows from the Nullstellensatz as in the proof of Lemma 9. □

Remarks. (a) Suppose that k is of characteristic $p > 0$. Let V be an elementary abelian group of order p^n for $n \geq 2$, and let X be a subgroup of order at least p^2. If W is a subgroup of V of index p, then $W \cap X$ is non-trivial, and so the number of elements in the intersection of X with any coset of W is divisible by p. Thus $\sum_{v \in X} v$ lies in $I(W)kV$.
(b) When the characteristic of F is zero, Proposition 3 is also valid for other actions on A by a group Q. The given argument applies as long as the induced orbit of any non-zero element of the $\mathbb{Q}$-dual of F^n does not lie in a finite union of hyperplanes; one just requires an α^g not in the annihilator of any element of Y. However, when the characteristic of F is non-zero, one does need such an orbit to satisfy a density property analogous to that of Lemma 10.

References

[1] BOURBAKI, *Commutative algebra* (Hermann, 1972).

[2] ALAN R. CAMINA and DAVID M. EVANS, Some infinite permutation modules, *Quart. J. Math. Oxford* (2), **42** (1991), 15–26.

[3] DANIEL R. FARKAS and ROBERT L. SNIDER, Simple augmentation modules, *Quart. J. Math. Oxford* (2), **45** (1994), 29–42.

[4] N. JACOBSON, *Structure of rings* (American Math. Soc., 1964, 2nd edition).