TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 354, Number 8, Pages 3379–3408
S 0002-9947(02)03006-4
Article electronically published on April 1, 2002

INVARIANT IDEALS AND POLYNOMIAL FORMS

D. S. PASSMAN

Dedicated to Idun Reiten on the occasion of her 60th birthday

ABSTRACT. Let $K[\mathfrak{H}]$ denote the group algebra of an infinite locally finite group $\mathfrak{H}$. In recent years, the lattice of ideals of $K[\mathfrak{H}]$ has been extensively studied under the assumption that $\mathfrak{H}$ is simple. From these many results, it appears that such group algebras tend to have very few ideals. While some work still remains to be done in the simple group case, we nevertheless move on to the next stage of this program by considering certain abelian-by-(quasi-simple) groups. Standard arguments reduce this problem to that of characterizing the ideals of an abelian group algebra $K[V]$ stable under the action of an appropriate automorphism group of V. Specifically, in this paper, we let $\mathfrak{G}$ be a quasi-simple group of Lie type defined over an infinite locally finite field F, and we let V be a finite-dimensional vector space over a field E of the same characteristic p. If $\mathfrak{G}$ acts nontrivially on V by way of the homomorphism $\phi\colon \mathfrak{G} \to \mathrm{GL}(V)$, and if V has no proper $\mathfrak{G}$-stable subgroups, then we show that the augmentation ideal $\omega K[V]$ is the unique proper $\mathfrak{G}$-stable ideal of $K[V]$ when $\mathrm{char} K \neq p$. The proof of this result requires, among other things, that we study characteristic p division rings D, certain multiplicative subgroups G of $D^\bullet$, and the action of G on the group algebra $K[A]$, where A is the additive group D^+. In particular, properties of the quasi-simple group $\mathfrak{G}$ come into play only in the final section of this paper.

1. Introduction

If $\mathfrak{H}$ is a nonidentity group, then the group algebra $K[\mathfrak{H}]$ always has at least three distinct ideals, namely 0, the augmentation ideal $\omega K[\mathfrak{H}]$, and $K[\mathfrak{H}]$ itself. Thus it is natural to ask if groups exist for which the augmentation ideal is the unique nontrivial ideal. In such cases, one says that $\omega K[\mathfrak{H}]$ is *simple*. Certainly $\mathfrak{H}$ must be a simple group for this to occur; and, since the finite situation is easy enough to describe, we might as well assume that $\mathfrak{H}$ is infinite simple. The first such examples, namely algebraically closed groups and universal groups, were offered in [BHPS]. From this, it appeared that such groups would be quite rare. But A. E. Zalesskiĭ has shown that, for locally finite groups, this phenomenon is really the norm. Indeed, for all locally finite infinite simple groups, the characteristic 0 group algebras $K[\mathfrak{H}]$ tend to have very few ideals. See [Z4] for a survey of this material. Additional papers of interest include [HZ2], [LP], [Z2] and [Z3].

In a previous paper [PZ], A. E. Zalesskiĭ and this author studied the lattice of ideals of $K[\mathfrak{H}]$ in the obvious next generation of cases. These are the locally finite

Received by the editors November 16, 2001.
2000 *Mathematics Subject Classification.* Primary 16S34; Secondary 20F50, 20G05.
Research supported in part by NSF Grant DMS-9820271.

groups $\mathfrak{H}$ having a minimal normal abelian subgroup V with $\mathfrak{H}/V$ infinite simple (or perhaps just close to being simple). Note that $\mathfrak{G} = \mathfrak{H}/V$ acts as automorphisms on V, and hence on the group algebra $K[V]$. Furthermore, if I is any nonzero ideal of $K[\mathfrak{H}]$, then it is easy to see that $I \cap K[V]$ is a nonzero $\mathfrak{G}$-stable ideal of $K[V]$. Thus, for the most part, we were concerned with classifying these $\mathfrak{G}$-stable ideals. Even in concrete cases, this turned out to be a surprisingly difficult task. Note that the minimality of V implies that V contains no proper $\mathfrak{G}$-stable subgroup. As a natural starting point, we considered rational irreducible representations of quasi-simple groups of Lie type, and we showed

Proposition 1.1 ([PZ]). *Let $\mathfrak{G}$ be a quasi-simple group of Lie type defined over an infinite locally finite field F and let $\phi\colon \mathfrak{G} \to \mathrm{GL}(n, F)$ be a rational irreducible representation with F generated by the values of the group character associated to ϕ. If V is the $F[\mathfrak{G}]$-module determined by ϕ, and if K is a field of characteristic different from that of F, then $\omega K[V]$ is the unique proper $\mathfrak{G}$-stable ideal of $K[V]$.*

We remark that [BE] obtains an analogous result when $\mathfrak{G} = \mathrm{GL}(V)$ and F is an arbitrary infinite field. Furthermore, [OPZ, Example 3.9] considers $\mathrm{GL}(V)$ for finite-dimensional vector spaces over division rings.

Now suppose $\mathfrak{G}$, V and F are as in Proposition 1.1. Let $\operatorname{char} F = p > 0$ and let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{G}$. Then V contains a unique line L centralized by $\mathfrak{P}$, and, in the course of our proof, it was necessary to consider the action of a maximal torus $\mathfrak{T}$ on L and then on $K[L]$. Aspects of the latter situation turned out to be of interest in their own right and, jointly with J. M. Osterburg, we proved

Proposition 1.2 ([OPZ]). *Let D be an infinite division ring and let V be a finite-dimensional D-vector space. Furthermore, let $G = D^\bullet$ act on V and hence on the group algebra $K[V]$. Then every G-stable semiprime ideal of $K[V]$ can be written uniquely as a finite irredundant intersection $\bigcap_{i=1}^{k} \omega K[A_i]{\cdot}K[V]$, where each A_i is a D-subspace of V. As a consequence, the set of these G-stable semiprime ideals is Noetherian.*

In this paper, we complete the work of [PZ] by studying the nonrational representations of $\mathfrak{G}$, and our main result is

Main Theorem. *Let $\mathfrak{G}$ be a quasi-simple group of Lie type defined over an infinite locally finite field F of characteristic $p > 0$, and let V be a finite-dimensional vector space over a characteristic p field E. Assume that $\mathfrak{G}$ acts nontrivially on V by way of the representation $\phi\colon \mathfrak{G} \to \mathrm{GL}(V)$, and that V contains no proper $\mathfrak{G}$-stable subgroup. If K is a field of characteristic different from p, then $\omega K[V]$ is the unique proper $\mathfrak{G}$-stable ideal of the group algebra $K[V]$.*

Again, it is necessary to study the action of a maximal torus $\mathfrak{T}$ on $K[L]$, where L is a line in V, but this time more field automorphisms come into play. Indeed, we are faced with the following situation. Let F be an infinite locally finite field and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be $n \geq 1$ field automorphisms. Then the map $\theta\colon x \mapsto x^{\sigma_1} x^{\sigma_2} \cdots x^{\sigma_n}$ is an endomorphism of the multiplicative group $F^\bullet$, and we let G denote its image. Of course, G acts via multiplication on the additive group $A = F^+$ and hence on any group algebra $K[A]$. The goal is to determine the G-stable ideals of $K[A]$ under the additional assumption that G generates the field F.

Now, it is easy to construct examples where such a group G has infinite index in $F^\bullet$, so we cannot just use the methods of [PZ]. Instead, we take a somewhat different approach. The key here is not that G generates F, but surprisingly that the map $(x_1, x_2, \ldots, x_n) \mapsto x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n}$ is multilinear. This leads us to define the concept of a polynomial form and to show that such forms are eventually zero if the image is assumed to be finite. This is the content of Proposition 2.3, a result which shows up several times in the course of the proof of the main theorem. While we are not able to completely characterize all G-stable ideals of $K[A]$, we are able to obtain partial results and to successfully finesse the missing pieces.

This paper closes with the promised brief addendum to paper [OPZ]. Finally, the author would like to thank Professors J. M. Osterburg and A. E. Zalesskiĭ for their kind help on this project.

2. Polynomial Forms

Let $\mathfrak{Z}$ be a ring, let A be an infinite left $\mathfrak{Z}$-module and let S be a finite abelian group. For convenience, we let $\mathcal{I}(A)$ denote the set of infinite $\mathfrak{Z}$-submodules of A. In the following, we study arbitrary (not necessarily linear) functions $f\colon A \to S$. We say that such a function f is *eventually null* if every infinite submodule B of A contains an infinite submodule C with $f(C) = 0$. Obviously the zero function is eventually null, and so also is any group homomorphism whose kernel is a $\mathfrak{Z}$-submodule. Indeed, in the latter situation, the finiteness of S implies that $f^{-1}(0)$ is a submodule of finite index in A. We require the following trivial observation.

Lemma 2.1. *Let $\mathfrak{Z}$, A and S be as above, and let $B \in \mathcal{I}(A)$.*

(i) *If $f\colon A \to S$ is eventually null, then the restricted map $f_{|B}\colon B \to S$ is also eventually null.*
(ii) *Let $f_1, f_2, \ldots, f_m$ be finitely many eventually null functions from A to S. Then B has an infinite submodule C with $f_i(C) = 0$ for all i. In particular, the function $f_1 + f_2 + \cdots + f_m$ is eventually null.*

Proof. Part (i) is obvious, and part (ii) proceeds by induction on m. Indeed, since f_m is eventually null, we know that there exists $D \in \mathcal{I}(B)$ with $f_m(D) = 0$. Furthermore, by induction applied to D, there exists $C \in \mathcal{I}(D) \subseteq \mathcal{I}(B)$ with $f_i(C) = 0$ for $i = 1, 2, \ldots, m-1$. Thus $f_i(C) = 0$ for all i, and the lemma is proved. □

We will be concerned with functions which we call *polynomial forms* on A. By definition, a polynomial form of degree 0 is the zero function, and for $n \geq 1$, we say that $f\colon A \to S$ is a polynomial form of degree $\leq n$ if and only if

(i) $f(a) = 0$ implies that $f(\mathfrak{Z}a) = 0$, and
(ii) for each $a \in A$, the function $g_a(x) = f(a + x) - f(a) - f(x)$ is a finite sum of polynomial forms of degree $\leq n - 1$.

It is clear from (ii) above that the polynomial forms of degree ≤ 1 are precisely the group homomorphisms from A to S whose kernels are $\mathfrak{Z}$-submodules of A.

Lemma 2.2. *Let $\mathfrak{Z}$, A and S be as above.*

(i) *If $f\colon A \to S$ is a polynomial form of degree $\leq n$ and if $B \in \mathcal{I}(A)$, then the restricted function $f_{|B}\colon B \to S$ is also a polynomial form of degree $\leq n$.*
(ii) *If A has no proper submodules of finite index and if $f\colon A \to S$ is a polynomial form of degree $\leq n$, then $f(A) = 0$.*

(iii) *Let R be an infinite ring, fix $r_0, r_1, \dots, r_n \in R$, and let $\sigma_1, \sigma_2, \dots, \sigma_n$ be $n \geq 1$ endomorphisms of R. Let $\mathfrak{Z}$ be a central subring of R stable under each σ_i, and let $A = R^+$ be the additive subgroup of R, so that A is naturally a $\mathfrak{Z}$-module. If $\lambda\colon A \to S$ is a group homomorphism whose kernel is a $\mathfrak{Z}$-submodule of A, then the map $f\colon A \to S$ given by $f(x) = \lambda(r_0 x^{\sigma_1} r_1 x^{\sigma_2} r_2 \cdots r_{n-1} x^{\sigma_n} r_n)$ is a polynomial form on A of degree $\leq n$.*

Proof. All three parts follow easily by induction on n. For example, in (ii) we know that each g_a is the zero function. Hence the identity $f(a + x) = f(a) + f(x)$ holds for all $a, x \in A$. In other words, $f\colon A \to S$ is a group homomorphism. But then $|A : \ker f| = |f(A)| < \infty$, so $A = \ker f$ by assumption and the fact that $\ker f$ is closed under multiplication by $\mathfrak{Z}$. □

The key result here is

Proposition 2.3. *Let A be an infinite $\mathfrak{Z}$-module, let S be a finite abelian group, and let $f\colon A \to S$ be a polynomial form of degree $\leq n$. Then f is an eventually null function.*

Proof. We proceed by induction on n, the case $n = 0$ being trivial. Assume now that $n \geq 1$ and that the result holds for all forms of degree $\leq n - 1$. In view of Lemma 2.2(i), it suffices to show that $f(B) = 0$ for some $B \in \mathcal{I}(A)$, and we prove this in a series of steps.

Step 1. *We may suppose that $f(B) = f(A)$ for all $B \in \mathcal{I}(A)$, so the goal is to show that $f(A) = 0$. Furthermore, we may assume that there exists $\gamma \in f(A)$ with $B \cap f^{-1}(\gamma)$ infinite for all $B \in \mathcal{I}(A)$.*

Proof. Since S is finite, we can choose an infinite submodule C of A so that $|f(C)|$ is minimal over all $|f(D)|$ with $D \in \mathcal{I}(A)$. By Lemma 2.2(i), it suffices to assume that $C = A$. In particular, the minimality of $|f(A)|$ implies that $f(B) = f(A)$ for all $B \in \mathcal{I}(A)$. The goal now is to show that $f(A) = 0$.

For the second part, suppose, by way of contradiction, that for each $C \in \mathcal{I}(A)$ and $\gamma \in f(A)$ there exists $D \in \mathcal{I}(C)$ with $D \cap f^{-1}(\gamma)$ finite. Label the elements of $f(A)$ as $\gamma_1, \gamma_2, \dots, \gamma_k$, and define the decreasing sequence $C_0 \supseteq C_1 \supseteq \cdots \supseteq C_k$ of infinite submodules of A inductively starting with $C_0 = A$. Furthermore, if $1 \leq i \leq k$ and if C_{i-1} is given, then we can take $C_i \in \mathcal{I}(C_{i-1})$ so that $C_i \cap f^{-1}(\gamma_i)$ is finite. It then follows that $C_k \cap f^{-1}(\gamma_i)$ is finite for all i, and this contradicts the fact that C_k is infinite while $f(A) \subseteq S$ is finite.

Thus there exist $C \in \mathcal{I}(A)$ and $\gamma \in f(A) = f(C)$ such that $D \cap f^{-1}(\gamma)$ is infinite for all $D \in \mathcal{I}(C)$. Replacing A by C if necessary, we can now assume that $B \cap f^{-1}(\gamma)$ is infinite for all $B \in \mathcal{I}(A)$. □

Step 2. *$f(A)$ is a subgroup of S, and $B \cap f^{-1}(\beta)$ is infinite for each $B \in \mathcal{I}(A)$ and $\beta \in f(A)$.*

Proof. For the first part, let $\alpha, \beta \in f(A)$ and fix $a \in A$ with $f(a) = \alpha$. By the definition of polynomial form, $g_a(x) = f(a + x) - f(a) - f(x)$ is a finite sum of polynomial forms of degree $\leq n - 1$. Since, by induction, each of these forms is eventually null, Lemma 2.1(ii) implies that g_a is eventually null. In particular, there exists $B \in \mathcal{I}(A)$ with $g_a(B) = 0$, and thus $0 = g_a(b) = f(a + b) - f(a) - f(b)$ for all $b \in B$. But $f(B) = f(A)$, by Step 1, so we can choose $b \in B$ with $f(b) = \beta$. It now follows that $f(a + b) = f(a) + f(b) = \alpha + \beta$, and consequently $\alpha + \beta \in f(A)$.

In other words, $f(A)$ is closed under addition, and therefore it is a subgroup of the finite group S.

The argument for the second part is similar. Let B be a fixed member of $\mathcal{I}(A)$, and let $\gamma \in f(A)$ be the element given by Step 1. Let $\alpha \in f(A) = f(B)$ be arbitrary and fix $a \in B$ with $f(a) = \alpha$. As above, there exists $C \in \mathcal{I}(B)$ such that $f(a+c) = f(a) + f(c)$ for all $c \in C$. Now $C \cap f^{-1}(\gamma)$ is infinite, by Step 1, so there are infinitely many distinct $c \in C$ with $f(c) = \gamma$. This then yields infinitely many $a + c \in B$ with $f(a+c) = f(a) + f(c) = \alpha + \gamma$. In other words, $B \cap f^{-1}(\alpha + \gamma)$ is infinite. But $\alpha \in f(A)$ is arbitrary and $f(A)$ is a group, so $\alpha+\gamma$ is also an arbitrary element of $f(A)$, and this step is proved. □

Step 3. *$f(A) = 0$, and the proposition is proved.*

Proof. Since $f(A) = f(B)$ for all $B \in \mathcal{I}(A)$, it suffices to find an infinite submodule B of A with $f(B) = 0$. Suppose by way of contradiction that no such B exists. We first show that if U is a finite submodule of A with $f(U) = 0$, then there exists a properly larger submodule U' of A with $f(U') = 0$. To this end, let U be given with $f(U) = 0$. Then, for each of the finitely many elements $u \in U$, we know that $g_u(x) = f(u+x) - f(u) - f(x)$ is a finite sum of polynomial forms of degree $\leq n-1$. Hence, by Lemma 2.1(ii) and induction, each g_u is an eventually null function. By Lemma 2.1(ii) again, there exists $B \in \mathcal{I}(A)$ with $g_u(B) = 0$ for all $u \in U$.

Since $f(U) = 0$, we have $0 \in f(A)$. Hence, by Step 2, we know that $B \cap f^{-1}(0)$ is infinite. In particular, since U is finite, we can choose $b \in B \cap f^{-1}(0)$ with $b \notin U$. Then $U' = \langle U, b \rangle = U + \mathfrak{Z}b$ is properly larger than U, and we claim that $f(U') = 0$. To this end, let $u+zb$ be an arbitrary element of $U' = U+\mathfrak{Z}b$ with $u \in U$ and $z \in \mathfrak{Z}$. Of course, $zb \in B$, and, by part (i) of the definition of a polynomial form, $f(b) = 0$ implies that $f(zb) = 0$. Thus, since $g_u(B) = 0$, we conclude that $f(u + zb) = f(u) + f(zb) = 0 + 0 = 0$, and $f(U')$ is indeed equal to 0.

We can now complete the proof. Note that $f(A)$ is a subgroup of S, so $0 \in f(A)$. Thus, by part (i) of the definition of a polynomial form, there exists a submodule V_0 of A with $f(V_0) = 0$. By assumption, V_0 must be finite, so the above implies that there exists a submodule $V_1 = V_0'$ properly larger than V_0 with $f(V_1) = 0$. Again, V_1 must be finite, so we can find a properly larger V_2 with $f(V_2) = 0$. Continuing in this manner, we obtain a strictly increasing sequence of submodules $V_0 \subset V_1 \subset V_2 \subset \cdots$ with $f(V_i) = 0$ for all i. But then $V = \bigcup_i V_i \in \mathcal{I}(A)$ and $f(V) = 0$, a contradiction. Thus A must have an infinite submodule B with $f(B) = 0$, and, as we observed, this proves the result. □

We now consider some examples with $\mathfrak{Z}$ the ring of integers, so that $\mathfrak{Z}$-modules are merely abelian groups. To start with, let A be an infinite abelian group, let S be a finite abelian group, and let $f\colon A \to S$ be a polynomial form of degree $\leq n$. If $n \leq 1$, then we know that A has a subgroup B of finite index with $f(B) = 0$. As we see below, this phenomenon does not extend to polynomial forms of larger degree.

Example 2.4. *Let F be an infinite field of characteristic $p > 0$ and assume that either*

(i) *$p > 2$ and F has an infinite proper subfield, or*
(ii) *$p = 2$ and F admits an automorphism σ of order 3.*

If $A = F^+$ is the additive subgroup of F, then there exists a polynomial form $f\colon A \to \mathrm{GF}(p)^+$ of degree ≤ 2 which does not vanish on any subgroup of A of finite index.

Proof. (i) Let K be the given infinite proper subfield of F and let $A = F^+ \supseteq K^+ = C$. Then A/C is a nontrivial elementary abelian p-group, so there exists a nonzero linear map $\lambda\colon A \to \mathrm{GF}(p)^+ = S$ with kernel $L \supseteq C$. Define $f\colon A \to S$ by $f(x) = \lambda(x^2)$, so that f is a polynomial form of degree ≤ 2 by Lemma 2.2(iii). Suppose, by way of contradiction, that there exists a subgroup B of finite index in A with $f(B) = 0$. In other words, $b^2 \in L$ for all $b \in B$.

Since $|C : B \cap C| < \infty$, we can write $C = U + (B \cap C)$ for some finite subgroup U of C. Now, for each $u \in U$, the difference function $g_u\colon A \to S$ given by $g_u(x) = f(u + x) - f(u) - f(x) = \lambda(2ux)$ is a group homomorphism with kernel D_u, a subgroup of finite index in A. Furthermore, since $u \in C = K^+$ and $L \supseteq C$, it follows that $D_u \supseteq C$. Thus $D = B \cap \bigcap_{u\in U} D_u$ is a subgroup of finite index in A containing $B \cap C$, and consequently $B' = U + D$ is a subgroup of finite index in A with $B' \supseteq U + (B \cap C) = C$. Next, we show that $f(B') = 0$. Indeed, let $b' = u + d$ be an arbitrary element of B' with $u \in U$ and $d \in D$. Then $d \in D \subseteq B$, so $f(d) = 0$. Furthermore, $u \in K$, so we have $u^2 \in K^+ = C \subseteq L$ and $f(u) = 0$. Finally, $d \in D_u$, so $0 = g_u(d) = f(u + d) - f(u) - f(d)$, and hence $f(b') = f(u + d) = f(u) + f(d) = 0 + 0 = 0$, as required.

Replacing B by B' if necessary, we may now suppose that $B \supseteq C$. Let $c \in C$ and $b \in B$ be arbitrary elements. Then $f(c + b)$, $f(c)$ and $f(b)$ are all zero, and hence $2cb = (c+b)^2 - c^2 - b^2 \in L$. Thus, since L is closed under addition and since $\operatorname{char} F \neq 2$, we have $L \supseteq (2K)B = KB$. But KB is certainly a K-subspace of A and, of course, $KB \supseteq B$. It follows that A/KB is a finite K-vector space, and, since K is infinite, we conclude that $A = KB \subseteq L$, a contradiction.

Note that, when $p = 2$, the map $f(x) = \lambda(x^2)$ is a group homomorphism, and consequently it does have a kernel of finite index in A.

(ii) The argument here applies in all prime characteristics p, but offers nothing new unless $p = 2$. Let $K = F_\sigma$ be the fixed field of σ, so that K is a proper infinite subfield of F with $(F : K) = 3$. Write $C = K^+$ and let $\lambda\colon A \to \mathrm{GF}(p)^+ = S$ be a nonzero linear map with $\ker \lambda = L \supseteq C$. Define $f\colon A \to S$ by $f(x) = \lambda(x^\sigma x^{\sigma^{-1}})$, so that f is a polynomial form of degree ≤ 2 by Lemma 2.2(iii). Suppose, by way of contradiction, that there exists a subgroup B of finite index in A with $f(B) = 0$. In other words, $b^\sigma b^{\sigma^{-1}} \in L$ for all $b \in B$. As in part (i), we can suppose that $B \supseteq C$.

Let $c \in C$ and $b \in B$ be arbitrary elements. Then $f(c+b)$, $f(c)$ and $f(b)$ are all zero, so, since c is fixed by σ, we have

$$c(b^\sigma + b^{\sigma^{-1}}) = (c+b)^\sigma (c+b)^{\sigma^{-1}} - c^\sigma c^{\sigma^{-1}} - b^\sigma b^{\sigma^{-1}} \in L.$$

Furthermore, since σ is a field automorphism of order 3, it follows that $b + b^\sigma + b^{\sigma^{-1}}$ and $c(b + b^\sigma + b^{\sigma^{-1}})$ are contained in the fixed field of σ and hence in $C \subseteq L$. Thus $cb = c(b + b^\sigma + b^{\sigma^{-1}}) - c(b^\sigma + b^{\sigma^{-1}}) \in L$, and we conclude that $L \supseteq KB$. As in (i), this yields the required contradiction. $\square$

Next, we can use finite fields to obtain some interesting constructions.

Lemma 2.5. *Let A be an infinite abelian group, let L be a finite field with additive group $S = L^+$, and let $\lambda\colon A \to S$ be a group homomorphism.*

(i) *For each $n \geq 1$ and each $s \in S$, the map $f\colon A \to S$ given by $f(x) = s\cdot\lambda(x)^n$ is a polynomial form of degree $\leq n$.*
(ii) *If $\mu\colon S \to S$ is any map with $\mu(0) = 0$, then the composite map $\mu \circ \lambda\colon A \to S$ is a finite sum of polynomial forms.*

Proof. Part (i) follows easily by induction on n, and part (ii) follows from (i) since any function $\mu\colon S \to S$ with $\mu(0) = 0$ can be written as a polynomial with zero constant term. □

As a consequence, we have

Example 2.6. *Let A be an infinite elementary abelian p-group. Then there exists a polynomial form $f\colon A \to S$ with $f(A)$ not a subgroup of S.*

Proof. If $p > 2$, let $\lambda\colon A \to \mathrm{GF}(p)^+ = S$ be any epimorphism and define $f(x) = \lambda(x)^{p-1}$. Then $f\colon A \to S$ is a polynomial form, by Lemma 2.5(i), and $f(A) = \{0, 1\}$ is not a subgroup of S. On the other hand, when $p = 2$ we let $\lambda\colon A \to \mathrm{GF}(2^4)^+ = S$ be an epimorphism and we set $f(x) = \lambda(x)^3$. Then $|f(A)| = 6$, so again $f(A)$ is not a subgroup of S. □

Again, let $\mathfrak{Z}$ be an arbitrary ring and let $f\colon A \to S$ be a polynomial form. Choose $f(B)$ to have minimum size over all submodules B of finite index in A. Then, for any submodule C of finite index in A, we have $f(C) \supseteq f(C \cap B) = f(B)$, since $C \cap B$ is a submodule of B having finite index in A. In other words, $f(B)$ is the unique minimum value over all such C, and we call $f(B)$ the *final value* of f. In view of the preceding example and Lemma 2.2(ii), it would be interesting to know whether the final value of a polynomial form f is necessarily a subgroup of S.

3. Invariant Ideals

Let D be an infinite division ring of characteristic $p > 0$, and let $A = D^+$ be its additive group, so that A is an infinite elementary abelian p-group. Furthermore, let K be a field of characteristic different from p, and let $\overline{K}$ denote its algebraic closure. If G is any subgroup of the multiplicative group $D^\bullet$, then G acts as automorphisms on A by right multiplication and hence G acts as automorphisms on the group algebras $K[A]$ and $\overline{K}[A]$. In particular, since $D \supseteq \mathrm{GF}(p)$, we see that $\mathrm{GF}(p)^\bullet$ acts on A and obviously gives rise to all the power automorphisms of A. Finally, if B is a finite subgroup of A, then we let $e_B = |B|^{-1}\sum_{b\in B} b \in K[B]$ denote the principal idempotent of $K[B] \subseteq \overline{K}[B]$. We list a number of basic observations below. Here, of course, $\omega K[A]$ denotes the augmentation ideal of $K[A]$.

Lemma 3.1. *With the above notation, let I be an ideal of $\overline{K}[A]$.*

(i) *$\overline{K}[A]/I$ is a commutative von Neumann regular ring, and therefore it is a semiprimitive ring.*
(ii) *Any irreducible representation of $\overline{K}[A]$ is merely an algebra homomorphism $\Lambda\colon \overline{K}[A] \to \overline{K}$ determined by a group homomorphism $\lambda\colon A \to \overline{K}^\bullet$.*
(iii) *If $I \not\subseteq \omega\overline{K}[A]$, then there exists a finite subgroup B of A with $e_B \in I$.*
(iv) *If $0 \neq I \subseteq \omega\overline{K}[A]$ and if I is $\mathrm{GF}(p)^\bullet$-stable, then there exist finite subgroups $B \supseteq C$ of A with $|B : C| = p$ and $e_C - e_B = e_C(1 - e_B) \in I$.*
(v) *If G is an infinite subgroup of $D^\bullet$, then $\overline{K}[A]$ is G-prime.*

Proof. (i) Since A is a locally finite abelian group having no elements of order equal to the characteristic of $\overline{K}$, we know that $\overline{K}[A]$ is a commutative von Neumann regular ring. Consequently, the same is true of any homomorphic image $\overline{K}[A]/I$.

(ii) Since $\overline{K}[A]$ is commutative, any irreducible representation must be a $\overline{K}$-algebra homomorphism $\Lambda\colon \overline{K}[A] \to T$, where T is a field extension of $\overline{K}$. But $\Lambda(A)$ consists of pth roots of unity, so $\Lambda(A) \subseteq \overline{K}^{\bullet}$ and hence $T = \overline{K}$.

(iii) Since $I \not\subseteq \omega\overline{K}[A]$, there certainly exists a finite subgroup B of A such that $I \cap \overline{K}[B] \not\subseteq \omega\overline{K}[B]$. The well-understood structure of ideals in $\overline{K}[B]$ now implies that $e_B \in I \cap \overline{K}[B] \subseteq I$.

(iv) Now $I \neq 0$, so there must exist a finite subgroup B of A and a primitive idempotent e of $\overline{K}[B]$ with $e \in I$. Note that e is nonprincipal since $I \subseteq \omega\overline{K}[A]$. Suppose e corresponds to the linear character $\mu\colon B \to \overline{K}^{\bullet}$, and let $C = \ker\mu$, so that $|B : C| = p$. Since I is $\mathrm{GF}(p)^{\bullet}$-stable, we know that $e' = \sum_{g\in\mathrm{GF}(p)^{\bullet}} e^g \in I$. But $\mathrm{GF}(p)^{\bullet}$ consists of all the power maps on B, and $|B/C| = p$. Thus, the corresponding linear characters μ^g are the $p-1$ nonprincipal linear characters of B with kernel C. In follows that $e' + e_B$ is the sum of all primitive idempotents of $\overline{K}[B]$ extending e_C. In other words, $e' + e_B = e_C$, and hence $e_C - e_B = e' \in I$. Of course, $e_C e_B = e_B$, so $e_C - e_B = e_C(1 - e_B)$ is a product of the idempotents e_C and $1 - e_B$.

(v) Form the group $H = A \rtimes G$, and suppose that I and J are G-stable ideals of $\overline{K}[A]$ with $IJ = 0$. Then $I' = I\cdot\overline{K}[H]$ and $J' = J\cdot\overline{K}[H]$ are two-sided ideals of $\overline{K}[H]$ with $I'J' = 0$. In particular, if $\Delta(H)$ is the finite conjugate (f.c.) center of H and if $\vartheta\colon \overline{K}[H] \to \overline{K}[\Delta(H)]$ denotes the natural projection, then [P, Theorem 4.2.9] implies that $\vartheta(I')\vartheta(J') = 0$ and hence that $\vartheta(I)\vartheta(J) = 0$. But G acts regularly on A and G is infinite, so $A \cap \Delta(H) = 1$ and $\overline{K}[A \cap \Delta(H)] = \overline{K}$. In particular, $\vartheta(I)\vartheta(J) = 0$ implies that either $\vartheta(I) = 0$ or $\vartheta(J) = 0$, and consequently that either $I = 0$ or $J = 0$. □

If L and B are subgroups of $A = D^+$, then we define the *residual* of L by B to be the subgroup

$$L_B = \{a \in A \mid Ba \subseteq L\} = \bigcap_{b\in B} b^{-1}L,$$

where we set $0^{-1}L = A$. It is clear that if both $|A : L| < \infty$ and $|B| < \infty$, then $|A : L_B| < \infty$. Furthermore, if $B \supseteq C$, then $L_B \subseteq L_C$. For the next result, we continue with the same notation, and recall that $D^{\bullet}$ acts on A and hence on the group algebra $\overline{K}[A]$.

Lemma 3.2. *Let $\Lambda\colon \overline{K}[A] \to \overline{K}$ be an algebra homomorphism corresponding to the group homomorphism $\lambda\colon A \to \overline{K}^{\bullet}$, and set $L = \ker\lambda$. Furthermore, let B be a finite subgroup of A and let $x \in D^{\bullet}$.*

(i) *$\Lambda((e_B)^x) \neq 0$ if and only if $x \in L_B$.*

(ii) *If C is a subgroup of B, then $\Lambda((e_C - e_B)^x) \neq 0$ if and only if $x \in L_C \setminus L_B$.*

Proof. (i) Since $(e_B)^x$ is the principal idempotent of the group algebra $\overline{K}[B^x]$, it follows that $\Lambda((e_B)^x) \neq 0$ if and only if the restriction of Λ to $\overline{K}[B^x]$ is the principal homomorphism. Of course, the latter occurs if and only if $B^x \subseteq \ker\lambda = L$, or equivalently if and only if $Bx \subseteq L$.

(ii) As we observed, $e_B e_C = e_B$, so $f = e_C - e_B = e_C(1 - e_B)$ is the product of the idempotents e_C and $1 - e_B$. In particular, since Λ maps any idempotent to either 0 or 1, $\Lambda(f^x) \neq 0$ if and only if $\Lambda((e_C)^x) \neq 0$ and $\Lambda((e_B)^x) = 0$. By (i), this occurs if and only if $x \in L_C \setminus L_B$. □

As a consequence of this and the main result of [OPZ], we have

Lemma 3.3. *Let $|A : L| = p$ and let $B \supseteq C$ be distinct finite subgroups of A. Then L_B is properly smaller than L_C.*

Proof. Since $|A/L| = p$, we can let $\Lambda \colon \overline{K}[A] \to \overline{K}$ be an algebra homomorphism corresponding to one of the $p-1$ linear characters $\lambda \colon A \to \overline{K}^\bullet$ with kernel L. Note that $e_B \neq e_C$, so $f = e_C - e_B$ is a nonzero element of $\overline{K}[A]$ contained in $\omega\overline{K}[A]$. Let $J = \sum_{x \in D^\bullet} f^x \overline{K}[A]$ be the $D^\bullet$-stable ideal of $\overline{K}[A]$ generated by f. Since $0 \neq J \subseteq \omega\overline{K}[A]$, Proposition 1.2 implies that $J = \omega\overline{K}[A]$. In particular, since Λ is not the principal homomorphism, it follows that $J \nsubseteq \ker \Lambda$. Thus, there exists $x \in D^\bullet$ with $\Lambda(f^x) \neq 0$. But $f^x = (e_C - e_B)^x$, so it follows from Lemma 3.2(ii) that $x \in L_C \setminus L_B$. □

If $G \subseteq D^\bullet$ acts on $K[A]$, then 0, $\omega K[A]$ and $K[A]$ are trivally G-invariant ideals of $K[A]$. All other ideals are considered to be nontrivial.

Proposition 3.4. *Let D, $A = D^+$ and K be as above. Furthermore, let G be a subgroup of $D^\bullet$, so that G acts as automorphisms on the group A, by right multiplication, and hence on $K[A]$.*

(i) *If $G \cap L \neq \emptyset$ for every subgroup L of finite index in A, then $K[A]$ has no nontrivial G-invariant ideals not contained in $\omega K[A]$.*
(ii) *If $G \cap (L + a) \neq \emptyset$ for every subgroup L of finite index in A and every element $a \in A$, then $K[A]$ has no nontrivial G-stable ideals contained in the augmentation ideal $\omega K[A]$.*

Proof. Let $\overline{K}$ denote the algebraic closure of K. If I is a nontrivial G-stable ideal of $K[A]$, then $\bar{I} = \overline{K} \otimes I$ is a nontrivial G-stable ideal of $\overline{K}[A]$. Furthermore, $I \subseteq \omega K[A]$ if and only if $\bar{I} \subseteq \omega\overline{K}[A]$. Thus, without loss of generality, we can assume that $K = \overline{K}$ is algebraically closed.

(i) Suppose I is a nontrivial G-stable ideal of $\overline{K}[A]$ not contained in $\omega\overline{K}[A]$. Since $I \neq 0$, Lemma 3.1(iii) implies that $e_B \in I$ for some finite subgroup $B \subseteq A$. Indeed, since I is G-stable, we have $(e_B)^x \in I$ for all $x \in G$. Furthermore, since $I \neq \overline{K}[A]$, Lemma 3.1(i)(ii) implies that there exists an algebra homomorphism $\Lambda \colon \overline{K}[A] \to \overline{K}$ with $\Lambda(I) = 0$. Let $\lambda \colon A \to \overline{K}^\bullet$ be the linear character associated with Λ, and set $L = \ker \lambda$. Then $|A : L| < \infty$, so $|A : L_B| < \infty$ and, by assumption, there exists $y \in G \cap L_B$. But then $\Lambda((e_B)^y) \neq 0$, by Lemma 3.2(i), and this contradicts the fact that $(e_B)^y \in I$.

(ii) Let $H = \mathrm{GF}(p)^\bullet$, so that H is a central subgroup of $D^\bullet$ of order $p-1$. Then H commutes with G, and we suppose first that J is a nontrivial GH-stable ideal of $\overline{K}[A]$ contained in $\omega\overline{K}[A]$. Since $J \neq 0$ is H-stable, Lemma 3.1(iv) implies that there exist finite subgroups $B \supseteq C$ of A such that $|B : C| = p$ and $e_C - e_B \in J$. Indeed, since J is G-stable, we have $(e_B - e_C)^x \in J$ for all $x \in G$. Note that J is properly smaller than $\omega\overline{K}[A]$, so it follows from Lemma 3.1(i)(ii) that there exists a nonprincipal algebra homomorphism $\Lambda \colon \overline{K}[A] \to \overline{K}$ with $\Lambda(J) = 0$. As usual, let $\lambda \colon A \to \overline{K}^\bullet$ be the nonprincipal linear character of A associated with Λ, and let $L = \ker \lambda$. Then $|A : L| = p$, so Lemma 3.3 implies that L_B is properly smaller than L_C. In particular, since $|A : L_B| < \infty$, it follows from the hypothesis that there exists $y \in G$ with $y \in L_C \setminus L_B$. But then $\Lambda((e_C - e_B)^y) \neq 0$, by Lemma 3.2(ii), and this contradicts the fact that $(e_C - e_B)^y \in J$. In other words, there are no nontrivial GH-stable ideals of $\overline{K}[A]$ contained in $\omega\overline{K}[A]$.

Finally, let I be a G-stable ideal of $\overline{K}[A]$ properly smaller than $\omega\overline{K}[A]$, and set $J = \bigcap_{h\in H} I^h$. Since G and H commute, each I^h is G-stable and hence J is a GH-stable ideal. But J is properly smaller than $\omega\overline{K}[A]$, so the above result implies that $J = 0$. In particular, we have $\prod_{h\in H} I^h = 0$, and, since $\overline{K}[A]$ is G-prime by Lemma 3.1(v), it follows that some I^h is equal to 0 and hence that $I = 0$. $\square$

We now move on to discuss particular groups G of interest. Specifically, let D be an infinite characteristic p division ring, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be $n \geq 1$ endomorphisms of D. Furthermore, fix a nonzero element $d \in D$ and consider the map

$$\theta\colon x \mapsto d{\cdot}x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$$

from D to D. Then $\theta(D^\bullet) \subseteq D^\bullet$ and, if B is any infinite subgroup of D^+, we let $G = G(B) = \langle\theta(B^\bullet)\rangle$ be the subgroup of $D^\bullet$ generated by $\theta(B^\bullet)$. Of course, G acts as automorphisms on the additive group $A = D^+$ by right multiplication, and hence G acts on any group algebra $K[A]$.

There is no gain in considering more general product expressions for θ, like $d_0x^{\sigma_1}d_1x^{\sigma_2}d_2\cdots d_{n-1}x^{\sigma_n}d_n$ with $0 \neq d_i \in D$. Indeed, if $0 \neq d \in D$ and if σ is an endomorphism of D, then $x^\sigma d = dd^{-1}x^\sigma d = dx^{\sigma d}$. Thus each of the d_i factors can be moved to the left at the expense of multiplying each σ_i by a suitable inner automorphism.

Theorem 3.5. *Let D, A, $G = G(B)$, and K be as above with D having characteristic $p > 0$. If $\operatorname{char} K \neq p$, then all proper G-stable ideals of $K[A]$ are contained in the augmentation ideal $\omega K[A]$. Furthermore, $\theta(B^\bullet)$ and $G(B)$ are infinite.*

Proof. View A as a module over the integers $\mathfrak{Z}$, let L be an arbitrary subgroup of finite index in the infinite group A, and let $\mu\colon A \to A/L = S$ be the natural epimorphism onto the finite group S. By Lemma 2.2(iii), the map $f\colon A \to S$ given by

$$f(x) = \mu(d{\cdot}x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n})$$

is a polynomial form of degree $\leq n$, and Proposition 2.3 implies that f is eventually null. In particular, B has an infinite subgroup C with $f(C) = 0$, and we can choose $c \in C \setminus 0$. Note that $g = d{\cdot}c^{\sigma_1}c^{\sigma_2}\cdots c^{\sigma_n} \in \theta(B^\bullet) \subseteq G$ and that $\mu(g) = f(c) = 0$. In other words, $g \in \theta(B^\bullet) \cap L$, so $G \cap L \neq \emptyset$. Since this holds for all such L, it is clear that $\theta(B^\bullet)$ is infinite, and Proposition 3.4(i) yields the result. $\square$

We remark that the preceding theorem holds in a more general context. Indeed, using essentially the same proof, one can show that if $G = G(B)$ acts on a right D-vector space V, then all proper G-stable ideals of $K[V]$ are contained in the augmentation ideal $\omega K[V]$.

Next, let F be an infinite field and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be $n \geq 1$ field endomorphisms of F. Then the map $\theta\colon x \mapsto x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$ is an endomorphism of the multiplicative group $F^\bullet$, and we can let $G = \theta(F^\bullet)$ denote its image. In this special case, with $B = F^+$, Theorem 3.5 yields

Corollary 3.6. *Let A, G and K be as above for the field F of characteristic $p > 0$. If $\operatorname{char} K \neq p$, then all proper G-stable ideals of $K[A]$ are contained in the augmentation ideal $\omega K[A]$. Furthermore, G is infinite.*

Note that neither of the preceding two results require that G generate the division ring, but such an assumption is surely needed to eliminate proper ideals contained in the augmentation ideal $\omega K[A]$. On the other hand, as we will see in an example below, G merely generating D is not sufficient to guarantee the above conclusions. We start with

Lemma 3.7. *Let D be a division ring of characteristic $p > 0$, set $A = D^+$, and let G be a subgroup of $D^\bullet$. As usual, G acts on A by right multiplication, and hence on $K[A]$, where K is a field of characteristic different from p. If there exists a subgroup L of A of index p with $G \cap L = \emptyset$, then $K[A]$ has a proper G-stable ideal not contained in $\omega K[A]$.*

Proof. Since $1 \in G$ and $G \cap L = \emptyset$, we have $1 \notin L$. Thus, since $|A : L| = p$, it follows that $A = L \oplus B$, where $B = \mathrm{GF}(p)^+$. Let I be the ideal of $K[A]$ generated by all $(e_B)^g$ with $g \in G$. Then surely I is a G-stable ideal of $K[A]$ not contained in $\omega K[A]$, and it suffices to show that $I \neq K[A]$. To this end, note that A/L is cyclic of order p, so there exists a group homomorphism $\lambda\colon A \to \overline{K}^\bullet$ with $\ker \lambda = L$. Furthermore, λ determines a nontrivial algebra homomorphism $\Lambda\colon \overline{K}[A] \to \overline{K}$. Finally, since $B = \mathrm{GF}(p)^+$, it is clear that $L = L_B$. In particular, $G \cap L_B = G \cap L = \emptyset$, so Lemma 3.2(i) implies that $\Lambda((e_B)^g) = 0$ for all $g \in G$. Thus $\ker \Lambda \supseteq I$ and $I \neq K[A]$, as required. □

Next, we need

Lemma 3.8. *Let $E = \mathrm{GF}(p^n)$, let q be a prime different from p, and let H be the Sylow q-subgroup of $E^\bullet$. Assume that $|H| \geq q$, and that $|H| \geq 4$ if $q = 2$. Now let $F = \mathrm{GF}(p^{nq}) \supseteq E$ and let $G \supseteq H$ be the Sylow q-subgroup of $F^\bullet$. Then $|G| = q|H|$, and we have:*

- (i) *If $E = \mathrm{GF}(p)H$, then $F = \mathrm{GF}(p)G$.*
- (ii) *Suppose there exists an additive map $\lambda\colon E^+ \to \mathrm{GF}(p)^+$ with $H \cap \ker \lambda = \emptyset$. Then λ extends to an additive map $\lambda^*\colon F^+ \to \mathrm{GF}(p)^+$ with $G \cap \ker \lambda^* = \emptyset$.*

Proof. If $|H| = q^t$, then $q^t = |p^n - 1|_q$ and, as is well known, the assumptions on $|H|$ imply that $q^{t+1} = |p^{nq} - 1|_q$. In particular, $|G| = q^{t+1} = q|H|$. Now let g be a generator of the cyclic group G, so that g is a root of the polynomial $f(\zeta) = \zeta^q - g^q \in E[\zeta]$. Since the degree $(F : E)$ is equal to the prime q and since $g \notin E$, we must have $f(\zeta)$ irreducible in $E[\zeta]$ and $F = E[g]$. It follows that $\{1, g, \ldots, g^{q-1}\}$ is an E-basis for F.

(i) By the above, we know that $F = EG$. Hence if $E = \mathrm{GF}(p)H$, then $F = \mathrm{GF}(p)HG = \mathrm{GF}(p)G$.

(ii) Now suppose that $\lambda\colon E^+ \to \mathrm{GF}(p)^+$ exists with $H \cap \ker \lambda = \emptyset$. Since every element $\alpha \in F$ can be written uniquely as $\alpha = \alpha_0 + \alpha_1 g + \cdots + \alpha_{q-1} g^{q-1}$ with $\alpha_i \in E$, we can define $\lambda^*\colon F^+ \to \mathrm{GF}(p)^+$ by

$$\lambda^*(\alpha) = \lambda(\alpha_0 + \alpha_1 + \cdots + \alpha_{q-1}).$$

Obviously λ^* is an additive homomorphism extending λ. Furthermore, note that $G = H \cup Hg \cup \cdots \cup Hg^{q-1}$, since $|G : H| = q$. In particular, any element of G can be written as hg^i, with $h \in H$ and $0 \le i \le q-1$, and then $\lambda^*(hg^i) = \lambda(h) \ne 0$ by assumption. In other words, $G \cap \ker \lambda^* = \emptyset$, and the lemma is proved. $\square$

As a consequence, we finally obtain

Example 3.9. *Let q be an odd prime. Then, for infinitely many primes $p \ne q$, there exists an infinite locally finite field F of characteristic $p > 0$ with q-primary subgroup G of $F^\bullet$ such that*

(i) *$F = \mathrm{GF}(p)G$ is generated by $\mathrm{GF}(p)$ and G, and*
(ii) *if $A = F^+$ and if K is any field of characteristic different from p, then there exists a proper G-stable ideal of the group algebra $K[A]$ not contained in $\omega K[A]$.*

Proof. Suppose q is an odd prime, and let $\Phi_1(\zeta) = 1 + \zeta + \cdots + \zeta^{q-1}$ and $\Phi_2(\zeta) = 1 + \zeta^q + \cdots + \zeta^{q(q-1)}$ be the cyclotomic polynomials of order q and q^2, respectively. Since $\Phi_2(\zeta)$ is irreducible in the integral polynomial ring $\mathbb{Z}[\zeta]$, the Frobenius Density Theorem (see [J, Theorem IV.5.2]) guarantees that it will remain irreducible in $\mathrm{GF}(p)[\zeta]$ for infinitely many primes p. Let $p > 2$ be any such prime, and note that $p \ne q$. Furthermore, since $\Phi_2(\zeta) = \Phi_1(\zeta^q)$, it is clear that $\Phi_1(\zeta)$ is also irreducible in $\mathrm{GF}(p)[\zeta]$. It follows from the latter that if h is an element of multiplicative order q in the algebraic closure of $\mathrm{GF}(p)$, then $E = \mathrm{GF}(p)[h]$ has $\{1, h, \ldots, h^{q-2}\}$ as a $\mathrm{GF}(p)$-basis and $h^{q-1} = -(1 + h + \cdots + h^{q-2})$. Furthermore, since $\Phi_2(\zeta)$ is also irreducible and since $\deg \Phi_2(\zeta) > \deg \Phi_1(\zeta)$, we see that E contains no elements of order q^2.

Thus $E = \mathrm{GF}(p^{q-1})$ is a finite field such that, if H is a Sylow q-subgroup of $E^\bullet$, then $H = \langle h \rangle$ has order q. As we observed, any element $\alpha \in E$ is uniquely writable as $\alpha = \alpha_0 + \alpha_1 h + \cdots + \alpha_{q-2} h^{q-2}$ with each $\alpha_i \in \mathrm{GF}(p)$, and we define the additive homomorphism $\lambda\colon E^+ \to \mathrm{GF}(p)^+$ by $\lambda(\alpha) = 2\alpha_0 + \alpha_1 + \cdots + \alpha_{q-2}$. Since $p > 2$, we have $\lambda(h^i) \ne 0$ for $i = 0, 1, \ldots, q-2$. Furthermore, $h^{q-1} = -(1 + h + \cdots + h^{q-2})$, so $\lambda(h^{q-1}) = -q \ne 0$ in $\mathrm{GF}(p)$. In other words, $H \cap \ker \lambda = \emptyset$, and of course $E = \mathrm{GF}(p)H$.

We can now apply both parts of Lemma 3.8 repeatedly to the chain of field extensions

$$E = \mathrm{GF}(p^{q-1}) \subseteq \mathrm{GF}(p^{(q-1)q}) \subseteq \mathrm{GF}(p^{(q-1)q^2}) \subseteq \cdots,$$

and we let $F = \bigcup_{i=0}^\infty \mathrm{GF}(p^{(q-1)q^i})$ be the union of this chain. Thus F is an infinite locally finite field, and it follows from Lemma 3.8(i) and induction that if G is the q-primary subgroup of $F^\bullet$, then $F = \mathrm{GF}(p)G$, so that F is generated by $\mathrm{GF}(p)$ and G. Furthermore, by Lemma 3.8(ii) and induction, there exists an additive homomorphism $\lambda^*\colon F^+ \to \mathrm{GF}(p)^+$ with $G \cap \ker \lambda^* = \emptyset$. Of course, $L = \ker \lambda^*$ is a subgroup of $A = F^+$ of index p, and since $L \cap G = \emptyset$, it is clear that Lemma 3.7 yields the result. $\square$

Note that, in the above argument, when $q = 3$ we can take $p = 5$ and $E = \mathrm{GF}(5^2)$, and when $q = 5$ we can take $p = 3$ and $E = \mathrm{GF}(3^4)$.

4. Configurations

As usual, let D be an infinite division ring of characteristic $p > 0$, set $A = D^+$, and let G be a multiplicative subgroup of $D^\bullet$. Then G acts as automorphisms on A by right multiplication, and hence G acts on any group algebra $K[A]$ with

$\operatorname{char} K \neq p$. We will be concerned with configurations of the following sort. Let I be a G-stable ideal of $K[A]$, and suppose there exists $\alpha \in K[A] \setminus I$ with $\alpha \cdot \omega K[T] \subseteq I$ for some subgroup T of finite index in A. In this situation, $K[A]/I$ has potentially interesting properties. For example, one can show in this generality that $K[A]/I$ contains primitive idempotents, a phenomenon that does not occur in $K[A]$. However, such results turn out to be irrelevant here since, for the groups G that are of interest to us, a configuration of this nature implies that $I = \omega K[A]$. Indeed, a stronger result will be proved in Theorem 4.7. We first discuss how such structures might arise.

Let V be an arbitrary group and let H act as automorphisms on V. Then H is said to act in a *unipotent* fashion on V if there exists a finite subnormal chain $1 = V_0 \triangleleft V_1 \triangleleft \cdots \triangleleft V_t = V$ of H-stable subgroups such that H acts trivially on each quotient V_{i+1}/V_i. The following two lemmas are slight variants of results in [RS] and [Z1], respectively.

Lemma 4.1. *Let H act in a unipotent manner on V, and let $J \subseteq I$ be H-stable ideals of the group ring $K[V]$. If $I \neq J$, then there exists an element $\alpha \in I \setminus J$ such that H centralizes α modulo J.*

Proof. Let $1 = V_0 \triangleleft V_1 \triangleleft \cdots \triangleleft V_t = V$ describe the unipotent action of H on V. We proceed by induction on t, the result being clear for $t = 0$ since $K[1] = K$. Assume the result holds for $t-1$, and choose $\gamma \in I \setminus J$ so that $\operatorname{supp} \gamma$ meets the minimal number, say $n+1$, of cosets of V_{t-1}. By replacing γ by γy^{-1} for some $y \in \operatorname{supp} \gamma$ if necessary, we can assume that $1 \in \operatorname{supp} \gamma$. Thus we can write $\gamma = \gamma_0 + \gamma_1 x_1 + \cdots + \gamma_n x_n$ with $0 \neq \gamma_i \in K[V_{t-1}]$ and with $1, x_1, \ldots, x_n$ in distinct cosets of V_{t-1}.

Now define

$$I' = \{\alpha_0 \mid \alpha = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n \in I \text{ with } \alpha_i \in K[V_{t-1}]\},$$
$$J' = \{\beta_0 \mid \beta = \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n \in J \text{ with } \beta_i \in K[V_{t-1}]\}.$$

Then I' and J' are ideals of $K[V_{t-1}]$, since $V_{t-1} \triangleleft V$, and $I' \supseteq J'$. Furthermore, since H acts trivially on V/V_{t-1}, we see that I' and J' are H-stable. Note also that in the above notation, if $\alpha_0 = \beta_0$, then $\alpha - \beta$ is an element of I whose support meets at most n cosets of V_{t-1}. Thus the minimality of $n+1$ implies that $\alpha - \beta \in J$ and hence that $\alpha \in J$. In particular, it now follows that $\gamma_0 \in I' \setminus J'$.

By induction, there exists an element $\alpha_0 \in I' \setminus J'$ centralized modulo J' by H, and let $\alpha = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n$ be its corresponding element in I. Then $\alpha_0 \notin J'$ implies that $\alpha \notin J$. Furthermore, if $g \in H$, then $\alpha^g - \alpha$ has its 0-term in J'. Thus, by the above remarks, $\alpha^g - \alpha \in J$, and hence H centralizes α modulo J. ◻

Suppose V is an arbitrary group and I is an ideal of the group algebra $K[V]$. If U is a normal subgroup of V, then $(I \cap K[U]) \cdot K[V]$ is an ideal of $K[V]$, and we say that U *controls* I whenever $I = (I \cap K[U]) \cdot K[V]$. In other words, this occurs precisely when $I \cap K[U]$ contains generators for I. It follows from [P, Lemma 8.1.1] that there exists a unique normal subgroup $\mathcal{C}(I)$, called the *controller* of I, with the property that $U \triangleleft V$ controls I if and only if $U \supseteq \mathcal{C}(I)$. In particular, if U_1 and U_2 control I, then so does their intersection $U_1 \cap U_2$. Furthermore, if H acts on V and stabilizes I, then H stabilizes $\mathcal{C}(I)$.

Lemma 4.2. *Let H act in a unipotent manner on the arbitrary group V with $Z = \mathbb{C}_V(H) \triangleleft V$, and let I be an H-stable ideal of $K[V]$. If I is not controlled by Z,* *then there exist an element $\alpha \in K[Z] \setminus (I \cap K[Z])$ and an element $v \in V \setminus Z$ having only finitely many H-conjugates modulo Z, such that $\alpha \cdot \omega K[T] \subseteq I \cap K[Z]$, where $T = \{v^{x-1} \mid x \in \mathbb{N}_H(vZ)\}$ is a subgroup of Z. Furthermore, for any $x, y \in \mathbb{N}_H(vZ)$, we have $v^{xy-1} = v^{x-1} \cdot v^{y-1}$.*

Proof. Let $L = I \cap K[Z]$, so that L is an ideal of $K[Z]$, and set $J = L \cdot K[V]$. We note that J is H-stable since H acts trivially on Z, and that J is properly smaller than I since, by assumption, I is not controlled by Z. Thus, since H acts in a unipotent manner on V, Lemma 4.1 implies that there exists an element $\alpha \in I \setminus J$ that is centralized modulo J by H.

Write $\alpha = \sum_{i=1}^{n} \alpha_i v_i$ with $\alpha_i \in K[Z]$ and with $\{v_1, v_2, \dots, v_n\}$ a set of coset representatives for distinct cosets of Z in V. If some $\alpha_i \in L$, then $\alpha_i v_i \in J$, and we can delete this term from α. Thus, it suffices to assume that $\alpha_i \in K[Z] \setminus L$ for all i. Furthermore, if $n = 1$, then $\alpha_1 = \alpha v_1^{-1} \in I \cap K[Z] = L$, a contradiction. Thus $n \geq 2$, and consequently we can assume that $v_1 \in V \setminus Z$.

If $g \in H$, then the ideal $J = L \cdot K[V]$ contains

$$\alpha - \alpha^g = \sum_i \alpha_i v_i - \sum_i \alpha_i v_i^g.$$

Since $\alpha_1 \notin L$, it follows that some term in the above sum, other than $\alpha_1 v_1$, also has support in the coset $v_1 Z$. In other words, there exists a subscript $j = j(g)$ with $v_j^g \in v_1 Z$ or equivalently with $v_1^{g^{-1}} \in v_j Z$. In particular, we see that v_1 has finitely many H-conjugates modulo Z.

Finally, if $g \in \mathbb{N}_H(v_1 Z)$, then $\alpha - \alpha^g \in L \cdot K[V]$ implies that $\alpha_1 v_1 - \alpha_1 v_1^g \in L \cdot K[V]$ and hence $\alpha_1(1 - v_1^g v_1^{-1}) \in L$. Thus $\alpha_1 \cdot \omega K[T] \subseteq L$, where T is the subgroup of Z generated by all v_1^{g-1} with $g \in \mathbb{N}_H(v_1 Z)$. Now note that if $x, y \in \mathbb{N}_H(v_1 Z)$, then $v_1^{x-1} \in Z$, so $v_1^{xy-y} = (v_1^{x-1})^y = v_1^{x-1}$ and hence $v_1^{xy-1} = v_1^{x-1} \cdot v_1^{y-1}$. In other words, the map $\mathbb{N}_H(v_1 Z) \to Z$ given by $x \mapsto v_1^{x-1}$ is a group homomorphism, and consequently $T = \{v_1^{g-1} \mid g \in \mathbb{N}_H(v_1 Z)\}$ is the image of this map. $\square$

If $Z = A$ and if $I \cap K[Z]$ is a G-stable ideal of $K[Z]$, then the preceding result does indeed yield an appropriate configuration. We now begin working towards the proof of Theorem 4.7. Recall that D is an infinite division ring of characteristic $p > 0$ and that $A = D^+$ is its additive group.

Lemma 4.3. *Let L be a proper subgroup of A of finite index.*

(i) *If $E = \{x \in D \mid Lx \subseteq L\}$, then E is a finite subfield of D with $|E| \leq |A : L|$.*
(ii) *If T is a subgroup of finite index in A, then the set $E' = \{x \in D \mid Tx \subseteq L\}$ is finite.*

Proof. (i) It is clear that E is closed under addition and multiplication, and that $0, 1 \in E$. Furthermore, if $0 \neq x \in E$, then $Ax = A$ yields $|A : Lx| = |Ax : Lx| = |A : L| < \infty$. Thus since $Lx \subseteq L$, it follows that $Lx = L$ and hence that $x^{-1} \in E$. In other words, E is a subdivision ring of D and L is a right E-subspace of A. But then A/L is an E-vector space and, since $0 \neq A/L$ is finite, we conclude that E is finite with $|E| \leq |A/L|$. By Wedderburn's theorem, E must be a finite field.

(ii) If $0 \neq x \in E'$, then $Tx \subseteq L$ implies that $T \subseteq Lx^{-1}$, and therefore Lx^{-1} is one of the finitely many subgroups of A containing T. In particular, if E' is infinite, then there exists an infinite subset X of $E' \setminus 0$ with $Lx^{-1} = Ly^{-1}$ for all $x, y \in X$. Thus $Lx^{-1}y = L$, and consequently $x_0^{-1} X \subseteq E$, where x_0 is any fixed element of X. Of course, this is a contradiction, since E is finite and X is infinite. $\square$

Again, we let K be a field of characteristic different from p, and we let $\overline{K}$ denote its algebraic closure. By Lemma 3.1(ii), we know that any irreducible representation of $\overline{K}[A]$ is an algebra homomorphism $\Lambda\colon \overline{K}[A] \to \overline{K}$ determined by a group homomorphism $\lambda\colon A \to \overline{K}^{\bullet}$. One such Λ is the principal representation given by $\lambda(A) = 1$, while for all over representations we have $|A : \ker\lambda| = p$. Since $D^{\bullet}$ acts on A, it permutes the irreducible representations of $\overline{K}[A]$. Specifically, if $x \in D^{\bullet}$, then Λ^x is the representation corresponding to $\lambda^x\colon A \to \overline{K}^{\bullet}$, where $\lambda^x(a) = \lambda(a^x)$ for all $a \in A$. Note that $\ker\lambda^x = (\ker\lambda)^{x^{-1}} = (\ker\lambda)x^{-1}$.

Recall that if L is a subgroup of A of finite index and if C is a finite subgroup of A, then the residual of L by C is defined to be

$$L_C = \{a \in A \mid Ca \subseteq L\}.$$

As we observed, the assumptions on L and C imply that L_C is a subgroup of finite index in A. Furthermore, if $\mathfrak{F}$ is a finite subfield of D and if C is a right $\mathfrak{F}$-subspace of A, then L_C is a left $\mathfrak{F}$-vector space. Indeed, if $a \in L_C$, then $C(\mathfrak{F}a) = (C\mathfrak{F})a \subseteq Ca \subseteq L$ and hence $\mathfrak{F}a \subseteq L_C$.

Lemma 4.4. *Let $\Lambda\colon \overline{K}[A] \to \overline{K}$ be an algebra homomorphism corresponding to the group homomorphism $\lambda\colon A \to \overline{K}^{\bullet}$, write $L = \ker\lambda$, and let $x, y \in D^{\bullet}$.*

(i) *If $\Lambda^x = \Lambda$, then either Λ is principal or $x = 1$.*
(ii) *If C is a finite subgroup of A and if $x - y \in L_C$, then Λ^x and Λ^y agree on the group algebra $\overline{K}[C]$.*

Proof. (i) If $\Lambda^x = \Lambda$, then $\lambda(a^x) = \lambda^x(a) = \lambda(a)$ for all $a \in A$. In additive notation, this means that $ax - a \in \ker\lambda = L$. In other words, we must have $A(x-1) \subseteq L$. But $x \neq 1$ implies that $A(x-1) = A$, so $A = L$ and Λ is principal.

(ii) Since $x - y \in L_C$, the definition of L_C implies that $C(x-y) \subseteq L$. In particular, for each $c \in C$, we have $cx - cy \in L = \ker\lambda$, so $\lambda(cx) = \lambda(cy)$. In multiplicative notation, this means that $\lambda^x(c) = \lambda(c^x) = \lambda(c^y) = \lambda^y(c)$, so λ^x and λ^y agree on C, as required. □

Now let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be $n \geq 1$ endomorphisms of D. Furthermore, fix $0 \neq d \in D$, and consider the map

$$\theta\colon x \mapsto d{\cdot}x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$$

from D to D. Then $\theta(D^{\bullet}) \subseteq D^{\bullet}$, since endomorphisms are necessarily one-to-one, and, if B is any infinite subgroup of $A = D^{+}$, we let $G = G(B) = \langle\theta(B^{\bullet})\rangle$ be the subgroup of $D^{\bullet}$ generated by $\theta(B^{\bullet})$. The following is a special case of Theorem 4.7 that does not require any additional assumptions on D.

Lemma 4.5. *Let $G = G(B)$ be as above and let I be a G-stable ideal of $K[A]$. Suppose there exists an element $\alpha \in K[A] \setminus I$ with $\alpha{\cdot}\omega K[T] \subseteq I$ for some subgroup T of finite index in A. If $\alpha \notin \omega K[A]$, then $I = \omega K[A]$.*

Proof. Let J be the set of all $\gamma \in K[A]$ such that $\gamma{\cdot}\omega K[C] \subseteq I$ for some subgroup C of finite index in A. Then it is easy to see that J is a G-stable ideal of $K[A]$. Furthermore, $\alpha \in J$, so $J \not\subseteq \omega K[A]$. Thus, by Theorem 3.5, $J = K[A]$ and hence $1 \in J$. In particular, $\omega K[C] = 1{\cdot}\omega K[C] \subseteq I$ for some subgroup C of finite index in A. Finally, let $\widetilde{C} = \{a \in A \mid 1 - a \in I\}$. Then $\widetilde{C}$ is a subgroup of A containing C, and $\widetilde{C}$ is easily seen to be G-stable. Since $|A : \widetilde{C}| < \infty$ and G is infinite, it follows from Lemma 4.3 with $L = \widetilde{C}$, that $\widetilde{C} = A$. Thus, $I \supseteq \omega K[A]$ and, since $I \neq K[A]$, the result follows. $\square$

At this point, it is necessary to introduce additional notation and hypotheses. To start with, we assume that the d-factor in θ is equal to 1, so that $\theta(x) = x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$. Next, we assume that there is a finite central subfield $\mathfrak{F}$ of D such that B is an infinite $\mathfrak{F}$-subspace of $A = D^+$ containing 1, and such that the endomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$ stabilize $\mathfrak{F}$. For convenience, if τ is any subset of the set $\eta = \{1, 2, \ldots, n\}$, let us write $\theta_\tau(x) = x^{\sigma_{i_1}}x^{\sigma_{i_2}}\cdots x^{\sigma_{i_t}}$, where $i_1 < i_2 < \cdots < i_t$ and $\{i_1, i_2, \ldots, i_t\} = \tau$. In particular, $\theta(x) = \theta_\eta(x)$, each $\theta_\tau \colon \mathfrak{F}^\bullet \to \mathfrak{F}^\bullet$ is a linear character of the group, and $\theta_\emptyset$ is the principal character. We say that τ is a proper subset of η if $\tau \neq \eta$, and we say that θ is $\mathfrak{F}$-*Galois free* if θ is not Galois conjugate, as a character of $\mathfrak{F}^\bullet$, to any θ_τ with τ a proper subset of η.

We must actually deal with finitely many copies of the above structure. Specifically, for each subscript $i = 1, 2, \ldots, t$, let us suppose we are given a map $\theta_i(x_i) = x_i^{\sigma_{i,1}}x_i^{\sigma_{i,2}}\cdots x_i^{\sigma_{i,n_i}}$ with $n_i \geq 1$. Next, assume that there is a central subfield $\mathfrak{F}$ of D stable under each endomorphism $\sigma_{i,j}$, and that there exist infinite $\mathfrak{F}$-subspaces $B_1, B_2, \ldots, B_t$ of A, each containing 1. We can then let $G = G(B_1, B_2, \ldots, B_t)$ be the subgroup of $D^\bullet$ generated by $\theta_1(B_1^\bullet)\theta_2(B_2^\bullet)\cdots\theta_t(B_t^\bullet)$, and we insist that each θ_i is $\mathfrak{F}$-Galois free. Again, this means that, as a character of $\mathfrak{F}^\bullet$, θ_i is not Galois conjugate to any factor θ_{i,τ_i}, with τ_i a proper subset of $\eta_i = \{1, 2, \ldots, n_i\}$.

Let us write $(\mathfrak{F}^\bullet)^t$ for the group which is the direct product of t copies of $\mathfrak{F}^\bullet$. Then for any subsets $\tau_i \subseteq \eta_i$, the function $y = (y_1, y_2, \ldots, y_t) \mapsto \prod_i \theta_{i,\tau_i}(y_i)$ defines a linear character of this group, namely a multiplicative homomorphism from $(\mathfrak{F}^\bullet)^t$ to $\mathfrak{F}^\bullet$. For convenience, if χ and ξ are linear characters of $(\mathfrak{F}^\bullet)^t$, then we use $[\chi, \xi] = \sum_{y \in (\mathfrak{F}^\bullet)^t} \chi(y)\xi(y^{-1})$ to denote the unnormalized character inner product. Then character orthogonality implies that $[\chi, \xi] = 0$ if $\chi \neq \xi$, while $[\chi, \chi] = |(\mathfrak{F}^\bullet)^t| = (|\mathfrak{F}| - 1)^t \equiv \pm 1 \mod p$. Of course, $[\ ,\ ]$ extends by linearity to a function on sums of characters.

Lemma 4.6. *Let $\mathfrak{F}$, $B_1, B_2, \ldots, B_t$, and $\theta_1, \theta_2, \ldots, \theta_t$ be as above.*

(i) *If L is an $\mathfrak{F}$-subspace of A of finite index and if $k \geq 1$, then there exist $\mathfrak{F}$-subspaces $X_i \subseteq B_i$, with $\prod_i \theta_i(1 + X_i) \subseteq L + 1$, where $\prod_i$ denotes the product in the natural order. Furthermore, we have $1 + X_i \subseteq B_i^\bullet$ for all i, the spaces $X_1, X_2, \ldots, X_{t-1}$ are finite with $\dim_{\mathfrak{F}} X_i \geq k$, and the space X_t is infinite dimensional.*

(ii) *If $X_1, X_2, \ldots, X_t$ are $\mathfrak{F}$-subspaces of $B_1, B_2, \ldots, B_t$, respectively, then the* $\mathrm{GF}(p)$*-linear span of $\prod_i \theta_i(1 + X_i)$ contains $\prod_i \theta_i(X_i)$.*

Proof. Using the preceding notation, it is clear that $\theta_i(1+x_i) = \sum_{\tau_i} \theta_{i,\tau_i}(x_i)$, where the sum is over all subsets τ_i of η_i.

(i) We show by induction on $1 \leq r \leq t$ that the result holds for the function $\prod_{i=1}^r \theta_i(x_i)$. Let $\lambda \colon A \to A/L = S$ be the natural homomorphism. We first consider the case $r = 1$. Since L is an $\mathfrak{F}$-subspace of A and $1 \in B_1$, it follows from Lemma 2.2(iii), with $\mathfrak{Z} = \mathfrak{F}$, that

$$f(\zeta) = \lambda\big(\theta_1(1 + \zeta) - 1\big) = \sum_{\tau_1 \neq \emptyset} \lambda\big(\theta_{1,\tau_1}(\zeta)\big)$$

is a finite sum of polynomial forms mapping B_1 to the finite group S. Thus, by Proposition 2.3 and Lemma 2.1(ii), $f(\zeta)$ is eventually null. In particular, there exists an infinite $\mathfrak{F}$-subspace X_1 of B_1 with $\lambda\big(\theta_1(1+X_1)-1\big)=0$, or equivalently with $\theta_1(1+X_1)-1\subseteq L$. Furthermore, by replacing X_1 by a subspace of codimension 1 if necessary, we can assume that $-1\notin X_1$. Thus $1+X_1\subseteq B_1^\bullet$, and this case is proved.

Now suppose the result holds for some $r<t$, and let $X_1, X_2, \dots, X_r$ be the corresponding subspaces obtained. Since X_r is infinite dimensional, we can replace it by a finite subspace of dimension at least k. In particular, $X=X_1\times X_2\times\cdots\times X_r$ is now finite. For each r-tuple $x=(x_1,x_2,\dots,x_r)\in X$ define

$$\begin{aligned} f_x(\zeta) &= \lambda\Big(\prod_{i=1}^{r}\theta_i(1+x_i)\cdot[\theta_{r+1}(1+\zeta)-1]\Big)\\ &= \sum_{\tau_{r+1}\neq\emptyset}\lambda\Big(\prod_{i=1}^{r}\theta_i(1+x_i)\cdot\theta_{r+1,\tau_{r+1}}(\zeta)\Big). \end{aligned}$$

Again, each f_x is a finite sum of polynomial forms on B_{r+1}, so each is eventually null by Proposition 2.3 and Lemma 2.1(ii). Furthermore, since there are only finitely many such functions, Lemma 2.1(ii) implies that there exists an infinite $\mathfrak{F}$-subspace $X_{r+1}\subseteq B_{r+1}$ with $f_x(X_{r+1})=0$ for all $x\in X$. As above, we can replace X_{r+1} by a subspace of codimension 1, if necessary, to guarantee that $1+X_{r+1}\subseteq B_{r+1}^\bullet$.

Finally, let $x_i\in X_i$ for $i=1,2,\dots,r+1$. Then, by induction, we know that $\prod_{i=1}^{r}\theta_i(1+x_i)-1\in L$. Furthermore, note that $f_x(x_{r+1})=0$ and hence we have $\prod_{i=1}^{r}\theta_i(1+x_i)\cdot[\theta_{r+1}(1+x_{r+1})-1]\in L$. Thus, by adding these two members of L, we obtain $\prod_{i=1}^{r+1}\theta_i(1+x_i)-1\in L$, and the induction step is proved. Of course, the result follows when $r=t$.

(ii) Let the product $\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}$ be viewed as a linear character of $(\mathfrak{F}^\bullet)^t$. If this character is Galois conjugate to $\theta_1\theta_2\cdots\theta_t$, then θ_{i,τ_i} must be Galois conjugate to θ_i, as a character of $\mathfrak{F}^\bullet$, for each i. By assumption, this can only occur if $\tau_i=\eta_i$ for all i. Now let Θ denote the sum of the distinct Galois conjugates of $\theta_1\theta_2\cdots\theta_t\colon(\mathfrak{F}^\bullet)^t\to\mathfrak{F}^\bullet$, so that $\Theta\big((\mathfrak{F}^\bullet)^t\big)\subseteq\mathrm{GF}(p)$. By the preceding comment and our observations on character orthogonality, we know that $[\Theta,\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}]=0$ unless $\tau_i=\eta_i$ for all i. Furthermore, since $\theta_1\theta_2\cdots\theta_t$ occurs in Θ with multiplicity 1, we have $[\Theta,\theta_1\theta_2\cdots\theta_t]=[\theta_1\theta_2\cdots\theta_t,\theta_1\theta_2\cdots\theta_t]=\pm1$.

Let $X=X_1\times X_2\times\cdots\times X_t$ and for each $x=(x_1,x_2,\dots,x_t)\in X$ write

$$\begin{aligned} \varphi(x) &= \theta_1(1+x_1)\theta_2(1+x_2)\cdots\theta_t(1+x_t)\\ &= \sum_{i,\tau_i}\theta_{1,\tau_1}(x_1)\theta_{2,\tau_2}(x_2)\cdots\theta_{t,\tau_t}(x_t), \end{aligned}$$

where the sum is over all subsets $\tau_i\subseteq\eta_i$ for all i. Next observe that if $x\in X$ and $y=(y_1,y_2,\dots,y_t)\in(\mathfrak{F}^\bullet)^t$, then $y^{-1}x=(y_1^{-1}x_1,y_2^{-1}x_2,\dots,y_t^{-1}x_t)\in X$ and

$$\begin{aligned} \varphi(y^{-1}x) &= \sum_{i,\tau_i}\theta_{1,\tau_1}(y_1^{-1}x_1)\theta_{2,\tau_2}(y_2^{-1}x_2)\cdots\theta_{t,\tau_t}(y_t^{-1}x_t)\\ &= \sum_{i,\tau_i}\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}(y^{-1})\cdot\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}(x). \end{aligned}$$

Thus, by using the inner products computed in the previous paragraph, we have

$$\begin{aligned}
&\sum_{y\in(\mathfrak{F}^\bullet)^t}\Theta(y)\varphi(y^{-1}x)\\
&\qquad=\sum_{i,\tau_i}\sum_{y\in(\mathfrak{F}^\bullet)^t}\Theta(y)\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}(y^{-1})\cdot\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}(x)\\
&\qquad=\sum_{i,\tau_i}[\Theta,\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}]\cdot\theta_{1,\tau_1}\theta_{2,\tau_2}\cdots\theta_{t,\tau_t}(x)\\
&\qquad=\pm\,\theta_1(x_1)\theta_2(x_2)\cdots\theta_t(x_t).
\end{aligned}$$

In particular, since $\sum_{y\in\mathfrak{F}^\bullet}\Theta(y)\varphi(y^{-1}x)$ is in the GF(p)-linear span of $\varphi(X)=\prod_i\theta_i(1+X_i)$, so is $\prod_i\theta_i(X_i)$. □

We can now easily prove the rather unwieldy main result of this section.

Theorem 4.7. *Let $\mathfrak{F}$ be a finite central subfield of the characteristic p division ring D, and let $B_1,B_2,\ldots,B_t$ be infinite $\mathfrak{F}$-subspaces of the additive group $A=D^+$, each containing 1. For each $i=1,2,\ldots,t$, let the map $\theta_i\colon D\to D$ be given by $\theta_i(x_i)=x_i^{\sigma_{i,1}}x_i^{\sigma_{i,2}}\cdots x_i^{\sigma_{i,n_i}}$ with $n_i\geq 1$. Here, the $\sigma_{i,j}$s are all endomorphisms of D that stabilize $\mathfrak{F}$, and we define $G=G(B_1,B_2,\ldots,B_t)$ to be the subgroup of $D^\bullet$ generated by the product $\theta_1(B_1^\bullet)\theta_2(B_2^\bullet)\cdots\theta_t(B_t^\bullet)$. Finally, let K be a field of characteristic different from p, let I be a G-stable ideal of $K[A]$, and suppose there exist an element $\alpha\in K[A]\setminus I$ and a subgroup T of A with $\alpha\cdot\omega K[T]\subseteq I$ and $|A:\widetilde{T}|<\infty$, where $\widetilde{T}$ is the subgroup of A generated by all $\theta_1(\mathfrak{F}^\bullet)\theta_2(\mathfrak{F}^\bullet)\cdots\theta_t(\mathfrak{F}^\bullet)$-conjugates of T. If each θ_i is $\mathfrak{F}$-Galois free, then $I=\omega K[A]$.*

Proof. Let us assume, to start with, that K is an algebraically closed field. Since $\alpha\in K[A]\setminus I$, it follows from Lemma 3.1(i)(ii) that there exists an irreducible representation $\Lambda\colon K[A]\to K$, determined by a group homomorphism $\lambda\colon A\to K^\bullet$, with $\Lambda(\alpha)\neq 0$ and $\Lambda(I)=0$. Let $L=\ker\lambda$, and let C be a finite subgroup of A containing the support of α. Since $\mathfrak{F}$ is finite, we can replace C by $C\mathfrak{F}$ if necessary to assume that C is an $\mathfrak{F}$-subspace of A. As we observed earlier, this implies that L_C is an $\mathfrak{F}$-subspace of A of finite index. Hence, by Lemma 4.6(i), there exist $\mathfrak{F}$-subspaces $X_i\subseteq B_i$, with $\prod_i\theta_i(1+X_i)\subseteq L_C+1$. Furthermore, $1+X_i\subseteq B_i^\bullet$ for all i, the spaces $X_1,X_2,\ldots,X_{t-1}$ are nonzero, and X_t is infinite.

Let $x=(x_1,x_2,\ldots,x_t)\in X=X_1\times X_2\times\cdots\times X_t$. Then $g=\prod_i\theta_i(1+x_i)\in G$ and, by applying g to the inclusion $\alpha\cdot\omega K[T]\subseteq I$, we obtain $\alpha^g\cdot\omega K[T^g]\subseteq I^g=I$. Thus $\Lambda(\alpha^g)\cdot\Lambda(\omega K[T^g])\subseteq\Lambda(I)=0$. But $g-1\in L_C$, so Lemma 4.4(ii) implies that Λ^g and $\Lambda^1=\Lambda$ agree on $K[C]$. In particular, $\Lambda(\alpha^g)=\Lambda^g(\alpha)=\Lambda(\alpha)\neq 0$, so $\Lambda(\omega K[T^g])=0$, and we deduce that $L=\ker\lambda\supseteq T^g=Tg=T\cdot\prod_i\theta_i(1+x_i)$. In other words, $L\supseteq T\cdot\prod_i\theta_i(1+X_i)$. Now we know from Lemma 4.6(ii), since each θ_i is $\mathfrak{F}$-Galois free, that the GF(p)-linear span of the set $\prod_i\theta_i(1+X_i)$ contains $\prod_i\theta_i(X_i)$. Thus, since T is a GF(p)-module, it follows that

$$L\supseteq T\cdot\prod_i\theta_i(X_i)=T\cdot\prod_i\theta_i(\mathfrak{F}^\bullet X_i)=T\cdot\prod_i\theta_i(\mathfrak{F}^\bullet)\cdot\prod_i\theta_i(X_i).$$

Of course, $\widetilde{T}$ is the linear span of $T\cdot\prod_i\theta_i(\mathfrak{F}^\bullet)$, and hence $L\supseteq\widetilde{T}\cdot\prod_i\theta_i(X_i)$. By assumption, $\widetilde{T}$ is a subgroup of finite index in A and, by Theorem 3.5, $\prod_i\theta_i(X_i)$ is infinite since $X_1,X_2,\ldots,X_{t-1}$ are nonzero and X_t is infinite. We can therefore conclude from Lemma 4.3(ii) that $L = A$. In other words, Λ can only be the principal representation of $K[A]$.

Now $\Lambda(\alpha) \neq 0$ and Λ is principal, so it follows that $\alpha \in K[A] \setminus \omega K[A]$. Thus, since $\omega K[A]$ is an $\mathfrak{F}^\bullet$-stable prime ideal of $K[A]$, we see that $\beta = \prod_{y \in \mathfrak{F}^\bullet} \alpha^y$ is also contained in $K[A] \setminus \omega K[A]$ and, of course, β is fixed by $\mathfrak{F}^\bullet$. Since $1 \in B_i$ for all i, it follows that $B_i \supseteq \mathfrak{F}$ and hence that $G \supseteq \theta_1(\mathfrak{F}^\bullet)\theta_2(\mathfrak{F}^\bullet) \cdots \theta_t(\mathfrak{F}^\bullet)$, a subgroup of $\mathfrak{F}^\bullet$. Thus I is stable under this subgroup, and therefore the inclusion $\beta \cdot \omega K[T] \subseteq I$ and the definition of $\widetilde{T}$ imply that $\beta \cdot \omega K[\widetilde{T}] \subseteq I$. Furthermore, by assumption, we have $|A : \widetilde{T}| < \infty$. Let $b_i \in B_i$ be fixed nonzero elements for $i = 1, 2, \ldots, t-1$. Then G contains the group $H = \langle d {\cdot} \theta_t(B_t) \rangle$, where $d = \prod_{i=1}^{t-1} \theta_i(b_i)$. Since $d \neq 0$, B_t is infinite, and I is H-stable, Lemma 4.5 implies that $I = \omega K[A]$, as required.

Finally, let K be arbitrary and, as usual, let $\overline{K}$ denote its algebraic closure. Then $\bar{I} = \overline{K} {\cdot} I$ is a G-stable ideal of $\overline{K}[A]$ with $\alpha \in \overline{K}[A] \setminus \bar{I}$ and $\alpha {\cdot} \omega \overline{K}[T] \subseteq \bar{I}$. By the algebraically closed result, we have $\bar{I} = \omega \overline{K}[A]$, and consequently $I = \bar{I} \cap K[A] = \omega \overline{K}[A] \cap K[A] = \omega K[A]$. $\square$

5. Locally Finite Fields

At this point, we shift our attention from arbitrary characteristic p division rings to (commutative) absolute fields. Recall that a field F is *locally finite* or *absolute* if every finite subset generates a finite subfield. In other words, F is locally finite of characteristic $p > 0$ precisely when it is a subfield of the algebraic closure of $\mathrm{GF}(p)$. Now let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be automorphisms of F. We say that $\theta(x) = x^{\sigma_1} x^{\sigma_2} \cdots x^{\sigma_n}$ is *p-bounded* if for every field automorphism π there are at most $p-1$ subscripts i with $\sigma_i = \pi$. Furthermore, we let $\mathfrak{f}$ denote the Frobenius, namely the field automorphism given by $x \mapsto x^p$. The following two lemmas yield an alternate approach to the work of [S, Section 2] in the case of locally finite fields. Here $\sigma\langle \mathfrak{f} \rangle$ denotes the σ-coset of the cyclic group $\langle \mathfrak{f} \rangle$.

Lemma 5.1. *Let F be a locally finite field of characteristic $p > 0$, and let θ be as above. Then there exists a p-bounded map $\xi(x) = x^{\kappa_1} x^{\kappa_2} \cdots x^{\kappa_m}$, determined by the field automorphisms $\kappa_1, \kappa_2, \ldots, \kappa_m$, such that*

(i) *$\theta(x) = \xi(x)$ for all $x \in F$, and*
(ii) *$\{\sigma_i \langle \mathfrak{f} \rangle \mid i = 1, 2, \ldots, n\} = \{\kappa_j \langle \mathfrak{f} \rangle \mid j = 1, 2, \ldots, m\}$.*

Proof. Suppose first that $F = \mathrm{GF}(p^k)$ is finite. Then we know that every field automorphism of F is uniquely of the form $\mathfrak{f}^r \colon x \mapsto x^{p^r}$ with $0 \leq r \leq k-1$. Hence $\theta(x) = x^v$ for some integer $v \geq 0$. Furthermore, since every element of F satisfies $x^{p^k} = x$, we can assume that $v \leq p^k - 1$. Thus, we can write $v = v_0 + v_1 p + \cdots + v_{k-1} p^{k-1}$ in its base p expansion with $0 \leq v_i \leq p-1$ for all i, and then $\xi(x) = \prod_{r=0}^{p-1} (x^{\mathfrak{f}^r})^{v_r}$ has the necessary properties.

Now let F be infinite, so that $\mathfrak{f}$ is an automorphism of infinite order. For convenience, let us assume that $\sigma_1, \sigma_2, \ldots, \sigma_m$ are the "smallest" σ elements in the cosets $\{\sigma_i \langle \mathfrak{f} \rangle \mid i = 1, 2, \ldots, n\}$. By this we mean that each σ_j can be written uniquely as $\sigma_i \mathfrak{f}^s$ with $s \geq 0$ and $i \in \{1, 2, \ldots, m\}$. Thus, $\theta(x) = \prod_{i=1}^m (x^{\sigma_i})^{a_i}$ with $a_i \geq 0$, and we write each a_i in its base p expansion as $a_i = \sum_{r=0}^t a_{i,r} p^r$ with $0 \leq a_{i,r} \leq p-1$. Then $\xi(x) = \prod_{i=1}^m \prod_{r=0}^t (x^{\sigma_i \mathfrak{f}^r})^{a_{i,r}}$ clearly has the appropriate properties. $\square$

These p-bounded maps are of importance to us because of the following uniqueness result. Note that here we view θ and ξ as maps on $F^\bullet$, rather than on the entire field F, and this requires the additional hypothesis in case F is a finite field.

Lemma 5.2. *Let $\theta(x) = x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$ and $\xi(x) = x^{\kappa_1}x^{\kappa_2}\cdots x^{\kappa_m}$ be p-bounded functions with $\theta(x) = \xi(x)$ for all $x \in F^\bullet$. Assume further that either $F = \mathrm{GF}(p^k)$ with $n, m < (p-1)k$, or that F is infinite. Then $n = m$ and, by relabeling if necessary, we have $\sigma_i = \kappa_i$ for all i.*

Proof. Suppose first that $F = \mathrm{GF}(p^k)$ is finite. For each integer $0 \le r \le k-1$, let $a_r = |\{i \mid \sigma_i = \mathfrak{f}^r\}|$ and let $b_r = |\{j \mid \kappa_j = \mathfrak{f}^r\}|$. Then $\theta(x) = x^a$ and $\xi(x) = x^b$, where $a = \sum_{r=0}^{k-1} a_r p^r$ and $b = \sum_{r=0}^{k-1} b_r p^r$. Note that $0 \le a_r, b_r \le p-1$, since both θ and ξ are p-bounded. Thus, since $n, m < (p-1)k$, we have $a, b < \sum_{r=0}^{k-1}(p-1)p^r = p^k - 1$. Now, $\theta(x) = \xi(x)$ for all $x \in F^\bullet$, so the polynomial $\zeta^a - \zeta^b \in \mathrm{GF}(p)[\zeta]$ has at least $p^k - 1$ roots. But $a, b < p^k - 1$, so this polynomial must be identically 0, and hence $a = b$. The uniqueness of the base p expansion now implies that $a_r = b_r$ for all r, and therefore the result follows in this case.

Finally, let F be an infinite locally finite field. If two automorphisms of F are distinct, then they differ on an element, and hence they differ when restricted to any finite subfield containing that element. We can therefore find a finite subfield $\mathfrak{F}$ of F such that any equality of the form $\sigma_i = \sigma_j$, $\sigma_i = \kappa_j$ or $\kappa_i = \kappa_j$ that holds in $\mathfrak{F}$, must also hold in F. Furthermore, we can assume that if $\mathfrak{F} = \mathrm{GF}(p^k)$, then $n, m < (p-1)k$. Since θ and ξ are both p-bounded and agree when restricted to $\mathfrak{F}^\bullet$, the finite field result implies that $n = m$ and that, by relabeling, we have $\sigma_i = \kappa_i$ as automorphisms of $\mathfrak{F}$. Thus $\sigma_i = \kappa_i$ as automorphisms of F. □

As a consequence, we obtain

Lemma 5.3. *Let $\theta(x) = x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$ be a p-bounded function on F with $n \ge 1$ and, if $F = \mathrm{GF}(p^k)$ is finite, assume in addition that $n < (p-1)k$.*

(i) *If F is finite, then θ is F-Galois free.*
(ii) *The linear span of $\theta(F^\bullet)$ is a subfield of F of finite index. Indeed, if π is an automorphism of F fixing $\theta(F^\bullet)$, then π has finite order and permutes the multiset $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ by right multiplication.*
(iii) *Suppose that F is an infinite field and that θ is an additive function when restricted to a subgroup L of finite index in $A = F^+$. Then we must have $n = 1$, so that $\theta(x) = x^{\sigma_1}$.*

Proof. (i) Let τ be a proper subset of $\eta = \{1, 2, \dots, n\}$, so that $|\tau| = m < n$, and let π be a field automorphism of F. Then θ_τ is a p-bounded function on F, and so also is θ^π. Thus, since $m, n < (p-1)k$ and $m \ne n$, we conclude from Lemma 5.2 that $\theta_\tau \ne \theta^\pi$ as characters of $F^\bullet$.

(ii) Since $\theta(F^\bullet)$ is a subgroup of $F^\bullet$, its linear span E is a subring of F. Hence E is a subfield of F, and the nature of F implies that F/E is a Galois extension. Now $\pi \in \mathrm{Gal}(F/E)$ if and only if θ^π and θ agree on $F^\bullet$. Thus, since θ^π is also p-bounded, we conclude from Lemma 5.2 again that $\theta^\pi = \theta$ if and only if $\{\sigma_1\pi, \sigma_2\pi, \dots, \sigma_n\pi\} = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ as multisets.

(iii) Let $\mathfrak{F}$ be any finite subfield of F. Since $|A : L| < \infty$ and $\mathfrak{F}$ is finite, we know that the residual $V = L_{\mathfrak{F}}$ is an $\mathfrak{F}$-subspace of A of finite index. In particular, V is nonzero since F is infinite, and $V \subseteq L$ since $1 \in \mathfrak{F}$. Fix $0 \ne v \in V$, and note that $\theta(yv) = \theta(y)\theta(v)$ for all $y \in \mathfrak{F}$. Thus, since θ is additive on V and $\theta(v) \ne 0$, we conclude that θ is additive on $\mathfrak{F}$. But F is the direct limit of all such finite subfields $\mathfrak{F}$, and hence θ is additive on F. Since θ is also multiplicative on F, it follows that it is an automorphism of the locally finite field. In other words, $\theta(x) = \xi(x)$ for all $x \in F$, where $\xi(x) = x^{\pi}$ for some automorphism π. Since ξ is certainly p-bounded, we conclude from Lemma 5.2 that $n = 1$ and that $\pi = \sigma_1$. $\square$

Additional applications of uniqueness include

Lemma 5.4. *Let F be an infinite absolute field and let $\theta(x) = x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$ be a function determined by $n \geq 1$ field automorphisms.*

(i) *If k is a positive integer, then the subfield of F spanned by $\theta(F^\bullet)$ is the same as the subfield spanned by $\theta^k(F^\bullet)$.*
(ii) *If E is the subfield of F spanned by $\theta(F^\bullet)$, then E must also be the linear span of $\theta(E^\bullet)$.*
(iii) *Let $\theta_1, \theta_2, \ldots, \theta_t$ be finitely many functions from F to F which, like θ, are determined by field automorphisms, and let E be the subfield of F spanned by the product $\theta_1(F^\bullet)\theta_2(F^\bullet)\cdots\theta_t(F^\bullet)$. Then E is also the linear span of $\theta_1(E^\bullet)\theta_2(E^\bullet)\cdots\theta_t(E^\bullet)$.*

Proof. (i) If E is the linear span of $\theta(F^\bullet)$ and if L is the linear span of $\theta^k(F^\bullet)$, then certainly $F \supseteq E \supseteq L$, and $(F : L) < \infty$ by Lemma 5.3(ii). Since all such extensions are Galois, it suffices to show that if π is an automorphism of F fixing $\theta^k(F^\bullet)$, then π fixes $\theta(F^\bullet)$.

By Lemma 5.1(i), it suffices to assume that θ is p-bounded; and, since L is a perfect field, we can assume that p does not divide k. Note that $\langle \mathfrak{f} \rangle$ is an infinite cyclic group since F is infinite. Now choose an integer $q > 0$ so that, for all i, j, if $\sigma_i\sigma_j^{-1} \in \langle \mathfrak{f} \rangle$ or if $\pi\sigma_i\sigma_j^{-1} \in \langle \mathfrak{f} \rangle$, then these finitely many terms are contained in $\{\mathfrak{f}^r \mid -q \leq r \leq q\}$. Since p is prime to k, there exists an integer $s > q$ with $p^s \equiv 1 \mod k$. Then $e = \sum_{m=0}^{k-1} p^{sm} \equiv k \equiv 0 \mod k$. In other words, k divides e, and hence π fixes $\theta^e(F^\bullet)$, where

$$\theta^e(x) = \Big(\prod_{i=1}^{n} x^{\sigma_i}\Big)^e = \prod_{i=1}^{n}\prod_{m=0}^{k-1} x^{\sigma_i \mathfrak{f}^{sm}}.$$

Since $s > q$, it follows easily that the latter expression describes a p-bounded formula for $\theta^e(x)$. Indeed, if $\sigma_i\mathfrak{f}^{sm_i} = \sigma_j\mathfrak{f}^{sm_j}$, then $\sigma_i\sigma_j^{-1} \in \langle \mathfrak{f} \rangle$; so we must have $m_i = m_j$ and $\sigma_i = \sigma_j$.

Next, since π fixes $\theta^e(F^\bullet)$, it follows from Lemma 5.3(ii) that π permutes the multiset $\{\sigma_i\mathfrak{f}^{sm} \mid 1 \leq i \leq n,\ 0 \leq m \leq k-1\}$. Again, since $s > q$, any equality of the form $\pi\sigma_i\mathfrak{f}^{sm_i} = \sigma_j\mathfrak{f}^{sm_j}$ implies that $m_i = m_j$ and $\pi\sigma_i = \sigma_j$. In other words, π permutes the multiset $\{\sigma_i \mid 1 \leq i \leq n\}$, and therefore Lemma 5.3(ii) implies that π fixes $\theta(F^\bullet)$.

(ii) By Lemma 5.3(ii), we know that $(F : E) = k < \infty$, and hence F/E is a finite Galois extension. Let $N\colon F \to E$ denote the norm map. Since $\theta(x)$ is multiplicative and since field automorphisms commute, the inclusion $\theta(F^\bullet) \subseteq E$ implies that $\theta\big(N(x)\big) = N\big(\theta(x)\big) = \theta^k(x)$ for all $x \in F^\bullet$. Thus, $\theta(F^\bullet) \supseteq \theta(E^\bullet) \supseteq \theta\big(N(F^\bullet)\big) \supseteq \theta^k(F^\bullet)$, and the result follows from (i).

(iii) Let E_i be the linear span of $\theta(F_i^\bullet)$, so that E is generated by the fields $E_1, E_2, \ldots, E_t$. By (ii), E_i is the linear span of $\theta_i(E_i^\bullet)$, and therefore the linear span of $\theta_i(E^\bullet)$ contains E_i. It follows that the linear span of $\theta_1(E^\bullet)\theta_2(E^\bullet)\cdots\theta_t(E^\bullet)$ contains $E_1E_2\cdots E_t = E$, as required. $\square$

We can now combine Theorem 4.7 with the above observations to obtain

Corollary 5.5. *Let F be an infinite locally finite field of characteristic p, set $A = F^+$, and, for each $i = 1, 2, \dots, t$, let the function $\theta_i\colon F \to F$ be given by $\theta_i(x_i) = x_i^{\sigma_{i,1}} x_i^{\sigma_{i,2}} \cdots x_i^{\sigma_{i,n_i}}$ with $n_i \geq 1$. Here, the $\sigma_{i,j}$s are all automorphisms of F, and we define $G = \theta_1(F^\bullet)\theta_2(F^\bullet)\cdots\theta_t(F^\bullet)$ so that G is a subgroup of $F^\bullet$. Finally, let K be a field of characteristic different from p, let I be a G-stable ideal of $K[A]$, and suppose there exist an element $\alpha \in K[A] \setminus I$ and a subgroup T of A with $\alpha \cdot \omega K[T] \subseteq I$ and $|A : \widetilde{T}| < \infty$, where $\widetilde{T}$ is a finite sum of $\theta_1(F^\bullet)\theta_2(F^\bullet)\cdots\theta_t(F^\bullet)$-conjugates of T. Then we must have $I = \omega K[A]$.*

Proof. By Lemma 5.1, it suffices to assume that $\theta_1, \theta_2, \dots, \theta_t$ are p-bounded functions on F. Thus, since F is an infinite locally finite field, we can find a finite subfield $\mathfrak{F} = \mathrm{GF}(p^k)$ of F such that:

(i) If $\sigma_{i,j} \neq \sigma_{i,j'}$ as automorphisms of F, then $\sigma_{i,j} \neq \sigma_{i,j'}$ as automorphisms of $\mathfrak{F}$.
(ii) $n_i < (p-1)k$ for all $i = 1, 2, \dots, t$.
(iii) $\widetilde{T}$ is a sum of $\theta_1(\mathfrak{F}^\bullet)\theta_2(\mathfrak{F}^\bullet)\cdots\theta_t(\mathfrak{F}^\bullet)$-conjugates of T.

Now it follows from (i), (ii) and Lemma 5.3(i) that each θ_i is $\mathfrak{F}$-Galois free. Furthermore, $A = F^+$ is an infinite $\mathfrak{F}$-space containing 1, and condition (iii) implies that $|A : \widetilde{T}| < \infty$, where $\widetilde{T}$ is a subgroup of A generated by $\theta_1(\mathfrak{F}^\bullet)\theta_2(\mathfrak{F}^\bullet)\cdots\theta_t(\mathfrak{F}^\bullet)$-conjugates of T. Thus, by Theorem 4.7, we conclude that $I = \omega K[A]$. $\square$

We will also need

Lemma 5.6. *Let F be an infinite locally finite field and let $\Psi(x)\colon F \to F$ be a map which can be written as a finite F-linear combination of functions of the form $\xi(x) = x^{\kappa_1} x^{\kappa_2} \cdots x^{\kappa_m}$, where each κ_i is a field automorphism. Assume, in addition, that $\Psi(0) = 0$.*

(i) *If $\Psi(F)$ is finite, then $\Psi(F) = 0$.*
(ii) *If $\Psi(x)$ is an additive map with $\Psi(F) \neq 0$, then F is a finite sum of F-translates of its additive subgroup $\Psi(F)$; that is, $F = \sum_{k=1}^n b_k \Psi(F)$ for suitable field elements $b_1, b_2, \dots, b_n$.*

Proof. Say $\Psi(x) = \sum_{i=1}^t a_i \xi_i(x)$ with $a_i \in F$. By combining terms if necessary, we can clearly assume that, as functions, the $\xi_i(x)$ are all distinct. In particular, there is at most one $\xi_i(x)$ given by the empty product and hence identically equal to 1. But then $\Psi(0) = 0$ implies that this term cannot appear in $\Psi(x)$. In other words, $\xi_i(0) = 0$ for all i, and hence, since these functions are distinct, they differ on nonzero elements. It follows that there exists a finite subfield $\mathfrak{F} \subseteq F$ such that the various $\xi_i(x)$ give rise to distinct linear characters $\xi_i\colon \mathfrak{F}^\bullet \to \mathfrak{F}^\bullet$.

For each $y \in \mathfrak{F}^\bullet$, define $\Psi_y(x) = \Psi(y^{-1}x)$ for all $x \in F$. Then

$$\Psi_y(x) = \sum_{i=1}^t a_i \xi_i(y^{-1}x) = \sum_{i=1}^t a_i \xi_i(y^{-1})\xi_i(x).$$

Thus, for any fixed subscript j, we have

$$\sum_{y \in \mathfrak{F}^\bullet} \xi_j(y)\Psi_y(x) = \sum_{i=1}^t \sum_{y \in \mathfrak{F}^\bullet} \xi_j(y)\xi_i(y^{-1}) \cdot a_i \xi_i(x) = \sum_{i=1}^t [\xi_j, \xi_i] \cdot a_i \xi_i(x),$$

where, as usual, $[\xi_j, \xi_i]$ denotes the unnormalized character inner product. In particular, character orthogonality yields

$$(*) \qquad \sum_{y \in \mathfrak{F}^\bullet} \xi_j(y)\Psi_y(x) = \pm a_j \xi_j(x) \qquad \text{for all } x \in F.$$

(i) If $\Psi(F)$ is finite, then each $\Psi_y(F)$ is finite, and hence, by the above, $a_j\xi_j(F)$ is finite. But $\xi_j(F)$ is infinite, by Theorem 3.5, and hence we must have $a_j = 0$ for all j. In other words, $\Psi(F) = 0$.

(ii) Now suppose that $\Psi(x)$ is additive with $\Psi(F) \neq 0$, and let the subscript j be chosen with $a_j \neq 0$. Since each $\Psi_y(x)$ is clearly also an additive function, it follows from $(*)$ that $a_j\xi_j(x)$ is additive and hence so is $\xi_j(x)$. Now, by Lemma 5.1(i), we can assume that $\xi_j(x)$ is p-bounded, and then, by Lemma 5.3(iii), it follows that $\xi_j(x)$ is an automorphism of F. In particular, $\xi_j(F) = F$, and hence $(*)$ yields

$$\sum_{y \in \mathfrak{F}^\bullet} \xi_j(y)\Psi(F) = \sum_{y \in \mathfrak{F}^\bullet} \xi_j(y)\Psi_y(F) \supseteq \pm a_j\xi_j(F) = F,$$

and the result follows. □

If $F = \overline{\mathrm{GF}(p)}$ is the algebraic closure of $\mathrm{GF}(p)$, then F has no proper subfield of finite index. Thus, by Lemma 5.3(ii), the linear span of $\theta(F^\bullet)$ is equal to F itself. On the other hand, if F admits an automorphism $\pi \neq 1$ of finite order n, then we can take $\theta(x) = xx^\pi \cdots x^{\pi^{n-1}}$ to be the norm map from F to F_π, the fixed field of π, and then $\theta(F^\bullet) \subseteq F_\pi$ with $(F : F_\pi) = n$. As we see below, it is possible for $\theta(F^\bullet)$ to span F and to have infinite index in the multiplicative group $F^\bullet$.

Example 5.7. *Let p be an odd prime, and let q be a prime divisor of $p-1$. Set $F = \bigcup_{n=0}^\infty \mathrm{GF}(p^{q^n})$, and assume that q^2 divides $p-1$ if $q = 2$. Then there exists a function $\theta(x) = x^{p-2}x^\sigma$, with σ an automorphism of F, such that $G = \theta(F^\bullet)$ is a q'-subgroup of $F^\bullet$. In particular, $|F^\bullet : G| = \infty$, even though F is the linear span of the group G.*

Proof. If q^a is the exact power of q dividing $p-1$, then, as is well known, the assumptions imply that q^{n+a} is the exact power of q dividing $p^{q^n}-1$. By induction, we construct automorphisms $\sigma_n = p^{k_n}$ of $\mathrm{GF}(p^{q^n})$ such that q^{a+n} divides $p-2+p^{k_n}$ and such that σ_{n+1} extends σ_n. To start with, take $\sigma_0 = p^0 = 1$. Now suppose that $\sigma_n = p^{k_n}$ exists. Since every element x of $\mathrm{GF}(p^{q^n})$ satisfies $x^{p^{q^n}} = x$, we can replace k_n by $k_{n+1} = k_n + bq^n$, for any nonnegative integer b, without changing the automorphism σ_n. We then define $\sigma_{n+1} = p^{k_{n+1}}$, and the goal is to find b so that q^{n+a+1} divides $p - 2 + p^{k_{n+1}}$.

Now we know that $p - 2 + p^{k_n} = \lambda q^{n+a}$ for some integer λ. Furthermore, $p^{q^n} = 1 + \mu q^{n+a}$, where q does not divide μ, and hence $p^{bq^n} \equiv 1 + b\mu q^{n+a} \mod q^{n+a+1}$ since $a \geq 1$. Thus

$$\begin{aligned} p - 2 + p^{k_{n+1}} &= \lambda q^{n+a} + p^{k_{n+1}} - p^{k_n} = \lambda q^{n+a} + p^{k_n}(p^{bq^n} - 1) \\ &\equiv q^{n+a}(\lambda + p^{k_n} b\mu) \mod q^{n+a+1}, \end{aligned}$$

and we need b to satisfy $\lambda + p^{k_n}b\mu \equiv 0 \mod q$. But $p \equiv 1 \mod q$, so this equation simplies to $\lambda + b\mu \equiv 0 \mod q$, and it has a nonnegative integer solution b since q does not divide μ.

Thus the sequence $\sigma_0, \sigma_1, \ldots$ can be constructed, and, since these automorphisms are consistent, they define an automorphism σ of $F = \bigcup_{n=0}^\infty \mathrm{GF}(p^{q^n})$. Finally, if

$x \in F^\bullet$ is a q-element of order dividing q^{n+a}, then $x \in \mathrm{GF}(p^{q^n})$, so $x^{p-2}x^\sigma = x^{p-2}x^{\sigma_n} = 1$ since q^{n+a} divides $p-2+p^{k_n}$. It follows that $\theta(F^\bullet)$ is a q'-group, and hence it has infinite index in $F^\bullet$. On the other hand, it is clear that F has no proper subfields of finite index. Thus, by Lemma 5.3(ii), we conclude that the linear span of $\theta(F^\bullet)$ is equal to F. □

Suppose F is an infinite locally finite field that admits an automorphism σ of order 2. Then it follows easily from Zsigmondy's Theorem that the kernel of the multiplicative norm map $\theta(x) = xx^\sigma$ contains elements of prime order for infinitely many different primes. Of course, $\theta(F^\bullet) = F_\sigma^\bullet$, where F_σ is the fixed field of σ.

6. Quasi-simple Groups of Lie Type

In this section, we prove our main result. To start with, we list properties of the representation $\phi\colon \mathfrak{G} \to \mathrm{GL}(V)$ which are needed for that argument. In order to handle the general situation of irreducible modules, rather than just absolutely irreducible ones, two fields seem to come into play. Here F is the field of definition of the group $\mathfrak{G}$, and E plays the role of the field of character values.

Hypothesis 6.1. *Let $F \supseteq E$ be infinite locally finite fields of characteristic $p > 0$, let V be a finite-dimensional E-vector space with $\dim_E V \geq 2$, and let $\mathfrak{G}$ be a group that acts on V by way of the homomorphism $\phi\colon \mathfrak{G} \to \mathrm{GL}(V)$. Assume that the following conditions are satisfied:*

(i) *$\mathfrak{P}$ is a p-subgroup of $\mathfrak{G}$ with $\mathbb{C}_V(\mathfrak{P}) = Ev_0$, and $Ev_0{\cdot}\phi(\mathfrak{G}) = V$.*

(ii) *$\mathfrak{T}$ is a subgroup of $\mathfrak{G}$ that stabilizes the line Ev_0, and the action of $\mathfrak{T}$ on this line factors through its homomorphic image $\overline{\mathfrak{T}} = (F^\bullet)^t = F^\bullet \times F^\bullet \times \cdots \times F^\bullet$. Indeed, for each $i = 1, 2, \ldots, t$, there exists a function $\theta_i\colon F \to E \subseteq F$ given by $\theta_i(x_i) = x_i^{\sigma_{i,1}} x_i^{\sigma_{i,2}} \cdots x_i^{\sigma_{i,n_i}}$ with*

$$v_0{\cdot}\overline{\phi}(x_1, x_2, \ldots, x_t) = \theta_1(x_1)\theta_2(x_2)\cdots\theta_t(x_t)v_0$$

for all $(x_1, x_2, \ldots, x_t) \in \overline{\mathfrak{T}}$. Here $\overline{\phi}$ denotes the induced action of $\overline{\mathfrak{T}}$ on v_0, each $n_i \geq 1$, and each $\sigma_{i,j}$ is a field automorphism of F. In addition, E is the linear span of the product $\theta_1(F^\bullet)\theta_2(F^\bullet)\cdots\theta_t(F^\bullet)$.

(iii) *$\mathfrak{P}$ is generated by one-parameter subgroups $\mathfrak{P}_g = \{g_x \mid x \in F\}$ such that the matrix entries of $\phi(g_x)$ are all F-linear sums of expressions of the form $x^{\kappa_1}x^{\kappa_2}\cdots x^{\kappa_m}$, where the κ_i are automorphisms of F and $m \geq 0$. Of course, these entries are contained in E, and $g_x{\cdot}g_y = g_{x+y}$ for all $x, y \in F$.*

As will be apparent, we have developed sufficient machinery to prove

Theorem 6.2. *Let $F \supseteq E$, V and $\mathfrak{G}$ satisfy Hypothesis 6.1, and let K be a field of characteristic different from p. Then the augmentation ideal $\omega K[V]$ is the unique proper $\mathfrak{G}$-stable ideal of the group algebra $K[V]$.*

Proof. Let I be a $\mathfrak{G}$-stable ideal of $K[V]$ different from 0 and $K[V]$. Our goal is to show that $I = \omega K[V]$.

Set $Z = Ev_0 = \mathbb{C}_V(\mathfrak{P})$, and note that $Z \cong A = E^+$. We first show that I is not controlled by Z. Suppose, by way of contradiction, that Z controls I, so that $Z \supseteq \mathcal{C}(I)$, the controller of I. Since $\mathcal{C}(I)$ is $\mathfrak{G}$-stable and since $Z{\cdot}\phi(\mathfrak{G}) = V \neq Z$, it follows that $\mathcal{C}(I)$ is properly smaller than Z. Furthermore, since the linear span of $\theta_1(F^\bullet)\theta_2(F^\bullet)\cdots\theta_t(F^\bullet)$ is equal to E, it is clear that $\mathfrak{T}$ stabilizes no proper subgroup of Z. In other words, we must have $\mathcal{C}(I) = \langle 1 \rangle$, in multiplicative notation, and consequently $I = (I \cap K) \cdot K[V] = 0$ or $K[V]$, a contradiction.

We now know that $Z = \mathbb{C}_V(\mathfrak{P})$ does not control I. In addition, since $\mathfrak{P}$ is a p-group, $\phi(\mathfrak{P})$ consists of unipotent elements and hence $\phi(\mathfrak{P})$ acts in a unipotent, that is, unitriangular, manner on the abelian group V. Thus, by Lemma 4.2, there exist an element $\alpha \in K[Z] \setminus (I \cap K[Z])$ and an element $v \in V \setminus Z$ having only finitely many $\mathfrak{P}$-conjugates modulo Z, such that $\alpha \cdot \omega K[T] \subseteq I \cap K[Z]$. Here, in multiplicative notation, $T = \{v^{h-1} \mid h \in \mathbb{N}_{\mathfrak{P}}(vZ)\}$ is a subgroup of Z. Furthermore, for all $g, h \in \mathbb{N}_{\mathfrak{P}}(vZ)$, we have $v^{gh-1} = v^{g-1} \cdot v^{h-1}$.

Next, we show that T is a "large" subgroup of Z. To start with, since $v \notin Z$ and since $\mathfrak{P}$ is generated by its one-parameter subgroups, there exists such a subgroup $\mathfrak{P}_g$ which does not centralize v. On the other hand, v has finitely many $\mathfrak{P}$-conjugates modulo Z, so it has finitely many $\mathfrak{P}_g$-conjugates modulo Z. Now extend v_0 to an E-basis $\{v_0, v_1, \ldots, v_\ell\}$ for V, and let $\Psi_i(x)\colon F \to E \subseteq F$ denote the v_i-coordinate of $v^{g_x-1} = v(\phi(g_x) - 1)$. By assumption, each $\Psi_i(x)$ is an F-linear combination of functions of the form $\xi(x) = x^{\kappa_1} x^{\kappa_2} \cdots x^{\kappa_m}$, where the κ_j are field automorphisms of F, and of course $\Psi_i(0) = 0$. Furthermore, since v has only finitely many $\mathfrak{P}_g$-conjugates modulo Z, we see that $\Psi_i(F)$ is finite for each $i \geq 1$. Thus, by Lemma 5.6(i), the $\Psi_i(x)$ with $i \geq 1$ are identically 0. It follows that $\mathbb{N}_{\mathfrak{P}_g}(vZ) = \mathfrak{P}_g$ and that $\Psi_0(x)$ is not identically 0, since otherwise $\mathfrak{P}_g$ would centralize v. Note also that, for all $x, y \in F$, we have

$$v_0^{g_{x+y}-1} = v_0^{g_x g_y - 1} = v_0^{g_x-1} \cdot v_0^{g_y-1},$$

and, in additive notation, this means that $\Psi_0(x+y) = \Psi_0(x) + \Psi_0(y)$. Thus, by Lemma 5.6(ii), there exist finitely many field elements $b_1, b_2, \ldots, b_r \in F$ such that $F = \sum_{i=1}^r b_i \Psi_0(F)$. Indeed, since $\Psi_0(F) \subseteq E$ and since F is free over E, there exist finitely many field elements $b'_1, b'_2, \ldots, b'_r \in E$ with $E = \sum_{i=1}^r b'_i \Psi_0(F)$. Hence, since $T \supseteq v\big(\phi(\mathfrak{P}_g) - 1\big) = \Psi_0(F) v_0$, we have

$$Z = E v_0 = \sum_{i=1}^r b'_i \Psi_0(F) v_0 \subseteq \sum_{i=1}^r b'_i T \subseteq Z.$$

But E is the linear span of $G = \theta_1(F^\bullet)\theta_2(F^\bullet) \cdots \theta_t(F^\bullet)$, so there exist finitely many elements $c_1, c_2, \ldots, c_s \in G$ with $Z = \sum_{j=1}^s c_j T$.

Finally, observe that $I \cap K[Z]$ is an ideal of $K[Z]$ stable under the action of $\theta_1(E^\bullet)\theta_2(E^\bullet) \cdots \theta_t(E^\bullet)$. Thus, since $Z \cong A = E^+$ and since the product $\theta_1(E^\bullet)\theta_2(E^\bullet) \cdots \theta_t(E^\bullet)$ spans E by Lemma 5.4(iii), Corollary 5.5 implies that $I \cap K[Z] = \omega K[Z]$. In other words, $I \supseteq \omega K[Z]$. But I is $\mathfrak{G}$-stable, so $I \supseteq \omega K[Z \cdot \phi(\mathfrak{G})] = \omega K[V]$, and the result follows. $\square$

It is an immediate consequence of the preceding theorem that there are no proper $\mathfrak{G}$-stable subgroups of V. But this is actually just a trivial exercise from the hypotheses, and it is essentially proved in Lemma 6.3(i).

Of course, it remains to show that the groups and modules we are interested in satisfy Hypothesis 6.1. For the most part, this is all spelled out in [PZ, Section 3], with appropriate references, so we can deal with this rather quickly. To this end, let $\mathfrak{G}$ denote a quasi-simple group of Lie type defined over an infinite locally finite field F of characteristic $p > 0$.

Lemma 6.3. *Let W be a finite-dimensional F-vector space on which $\mathfrak{G}$ acts both nontrivially and absolutely irreducibly. Then there exists a subfield E of F of finite index, and a $\mathfrak{G}$-stable E-subspace V of W such that*

(i) *V has no proper $\mathfrak{G}$-stable subgroup,*
(ii) *$W = F \otimes_E V$, and*
(iii) *$F \supseteq E$, V and $\mathfrak{G}$ satisfy Hypothesis 6.1.*

Proof. Let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{G}$ and let $\mathfrak{T}$ be a maximal torus of $\mathfrak{G}$ contained in $\mathbb{N}_{\mathfrak{G}}(\mathfrak{P})$. By [PZ, Theorem 3.1], a result of [BT] and [HZ1], we have $W = W_1^{\sigma_1} \otimes_F W_2^{\sigma_2} \otimes_F \cdots \otimes_F W_k^{\sigma_k}$, where each W_i is an infinitesimally irreducible $F[\mathfrak{G}]$-module and where each σ_i is a field automorphism. By the remarks following the above mentioned theorem in [PZ], $\mathfrak{P}$ centralizes a unique line Fw_0 in W. Indeed, $w_0 = w_1^{\sigma_1} \otimes w_2^{\sigma_2} \otimes \cdots \otimes w_k^{\sigma_k}$, where each w_i with $i \geq 1$ is a highest weight vector in W_i. Thus, by [PZ, Lemma 2.2], we see that $\mathfrak{T}$ acts on Fw_0 by way of certain functions $\theta_1, \theta_2, \ldots, \theta_t \colon F \to F$ as described in Hypothesis 6.1(ii). If E is the subfield of F spanned by the product $\theta_1(F^\bullet)\theta_2(F^\bullet)\cdots\theta_t(F^\bullet)$, then $(F : E) < \infty$ by Lemma 5.3(ii). Furthermore, by Lemma 5.4(iii), E is the linear span of the product $\theta_1(E^\bullet)\theta_2(E^\bullet)\cdots\theta_t(E^\bullet)$.

Now, according to [PZ, Lemma 3.3], E is equal to the field $\mathrm{GF}(p)[\chi]$ generated by all values $\chi(\mathfrak{G})$ of the corresponding group character $\chi \colon \mathfrak{G} \to F$. Thus, since $\mathfrak{G}$ is locally finite and $\operatorname{char} F = p > 0$, the representation associated with W is realizable over E. In other words, there exists a $\mathfrak{G}$-stable E-subspace $V \subseteq W$ with $W = F \otimes_E V$. This proves (ii), and of course $\mathfrak{G}$ must act nontrivially and irreducibly on ${}_EV$ since it acts nontrivially and irreducibly on ${}_FW$.

Since $\mathfrak{P}$ is a p-group, it acts in a unipotent manner on V, and hence $\mathbb{C}_V(\mathfrak{P}) \neq 0$. Indeed, since $F \otimes_E \mathbb{C}_V(\mathfrak{P}) \subseteq \mathbb{C}_W(\mathfrak{P})$, it follows that $\mathbb{C}_V(\mathfrak{P})$ is a line Ev_0 in V and, without loss of generality, we can assume that $w_0 = v_0 \in V$. With this, we now understand the action of $\mathfrak{T}$ on Ev_0. Furthermore, as can be seen for example in [C] or [St], $\mathfrak{P}$ is generated by one-parameter subgroups $\mathfrak{P}_g$ determined by root vectors, and each such subgroup acts on each W_i via polynomial maps. Of course, in the twisted cases, the defining field automorphism also comes into play. Thus, since $F \otimes_E V = W = W_1^{\sigma_1} \otimes_F W_2^{\sigma_2} \otimes_F \cdots \otimes_F W_k^{\sigma_k}$, we can now conclude that $F \supseteq E$, V and $\mathfrak{G}$ satisfy Hypothesis 6.1.

Finally, suppose U is a nonzero $\mathfrak{G}$-stable subgroup of V. Then $0 \neq \mathbb{C}_U(\mathfrak{P}) \subseteq \mathbb{C}_V(\mathfrak{P}) = Ev_0$. Furthermore, $\mathfrak{T}$ acts on $\mathbb{C}_U(\mathfrak{P})$ and, since E is the linear span of the product $\theta_1(E^\bullet)\theta_2(E^\bullet)\cdots\theta_t(E^\bullet)$, it follows that $\mathbb{C}_U(\mathfrak{P}) = Ev_0$. In particular, we have $U \supseteq Ev_0 \cdot \phi(\mathfrak{G}) = V$, and the proof is complete. □

It is now a simple matter to prove the Main Theorem, which, for convenience, we restate below.

Theorem 6.4. *Let $\mathfrak{G}$ be a quasi-simple group of Lie type defined over an infinite locally finite field F of characteristic $p > 0$, and let V be a finite-dimensional vector space over a characteristic p field E. Assume that $\mathfrak{G}$ acts nontrivially on V by way of the representation $\phi \colon \mathfrak{G} \to \mathrm{GL}(V)$, and that V contains no proper $\mathfrak{G}$-stable subgroup. If K is a field of characteristic different from p, then $\omega K[V]$ is the unique proper $\mathfrak{G}$-stable ideal of the group algebra $K[V]$.*

Proof. Since $\mathfrak{G}$ is a locally finite group and $\operatorname{char} E = p > 0$, we know that the representation $\phi \colon \mathfrak{G} \to \mathrm{GL}(V)$ is realizeable over the field $\mathrm{GF}(p)[\chi] \subseteq E$ generated by the character values $\chi(\mathfrak{G})$. Thus, since V contains no proper $\mathfrak{G}$-stable subgroup, we must have $E = \mathrm{GF}(p)[\chi] \subseteq \overline{\mathrm{GF}(p)}$, the algebraic closure of $\mathrm{GF}(p)$.

Now let $\overline{V} = \overline{\mathrm{GF}(p)} \otimes_E V$. Since V is a finite-dimensional irreducible $E[\mathfrak{G}]$-module, it follows that $\overline{V} = \overline{W}_1 \oplus \overline{W}_2 \oplus \cdots \oplus \overline{W}_k$ is a finite direct sum of absolutely irreducible $\overline{\mathrm{GF}(p)}[\mathfrak{G}]$-modules. Furthermore, by [PZ, Theorem 3.1], each $\overline{W}_i$ is isomorphic to $\overline{\mathrm{GF}(p)} \otimes_F W_i$, where W_i is an absolutely irreducible $F[\mathfrak{G}]$-module. In particular, by Lemma 6.3(ii), we have $W_i = F \otimes_{E_i} V_i$, where E_i is a subfield of finite index in F and where V_i is the $E_i[\mathfrak{G}]$-module given by that lemma. Thus $V \subseteq \overline{V} = \oplus \sum_{i=1}^{k} \overline{\mathrm{GF}(p)} \otimes_{E_i} V_i$, and the latter is isomorphic to a possibly infinite direct sum of the various V_i as $\mathrm{GF}(p)[\mathfrak{G}]$-modules. But V and each V_i is an irreducible $\mathrm{GF}(p)[\mathfrak{G}]$-module by Lemma 6.3(i), and hence we conclude that V is $\mathrm{GF}(p)[\mathfrak{G}]$-isomorphic to V_i for some i.

In other words, we can now assume that there exists an absolutely irreducible $F[\mathfrak{G}]$-module W such that $V \subseteq W$ is given by the preceding lemma. But then, by Lemma 6.3(iii), the triple $F \supseteq E$, V and $\mathfrak{G}$ satisfies Hypothesis 6.1, and consequently the result follows from Theorem 6.2. $\square$

Next, we paraphrase the above in terms of locally finite linear groups.

Corollary 6.5. *Let V be a finite-dimensional vector space over a field E of characteristic $p > 0$ and let $\mathfrak{G}$ be an infinite locally finite subgroup of $\mathrm{GL}(V)$. Assume that $\mathfrak{G}$ is quasi-simple and that it stabilizes no proper subgroup of V. If K is a field of characteristic different from p, then the augmentation ideal $\omega K[V]$ is the unique proper $\mathfrak{G}$-stable ideal of the group algebra $K[V]$.*

Proof. It essentially follows from the celebrated result of [Be], [Bo], [HS] and [T] that $\mathfrak{G}$ is a quasi-simple group of Lie type defined over an infinite locally finite field F of the same characteristic p. Now apply Theorem 6.4. $\square$

Finally, we return to the original problem of studying ideals in group algebras of locally finite abelian-by-simple groups. Recall that if V is a normal abelian subgroup of $\mathfrak{H}$, then $\mathfrak{H}/V$ acts on V by conjugation.

Corollary 6.6. *Let V be a finite-dimensional vector space over a field E of characteristic $p > 0$, and let V be a minimal normal abelian subgroup of the locally finite group $\mathfrak{H}$. Assume that $\mathfrak{H}/V$ is an infinite quasi-simple group that acts faithfully as a linear group on V. If K is a field of characteristic different from p and if I is a nonzero ideal of $K[\mathfrak{H}]$, then $I \supseteq \omega K[V]{\cdot}K[\mathfrak{H}]$, and hence I is the complete inverse image in $K[\mathfrak{H}]$ of an ideal of $K[\mathfrak{H}/V]$.*

Proof. Let $0 \neq I \triangleleft K[\mathfrak{H}]$ and suppose, by way of contradiction that $I \cap K[V] = 0$. Note that V acts in a unipotent manner on $\mathfrak{H}$, since it centralizes both V and $\mathfrak{H}/V$. Thus, since $\mathbb{C}_{\mathfrak{H}}(V) = V \triangleleft \mathfrak{H}$ and since V does not control I, it follows from Lemma 4.2 that there exist $0 \neq \alpha \in K[V]$ and $h \in \mathfrak{H} \setminus V$ with $\alpha{\cdot}\omega K[T] = 0$ and with $T = [h, V]$, the commutator group determined by the action of h on V. But T is a nonzero E-subspace of V, so T is infinite, and hence $\alpha{\cdot}\omega K[T] = 0$ implies that $\alpha = 0$, a contradiction.

We now know that $I \cap K[V]$ is a nonzero $\mathfrak{H}/V$-stable ideal of $K[V]$. Furthermore, since V is a minimal normal subgroup of $\mathfrak{H}$, it is clear that $\mathfrak{G} = \mathfrak{H}/V$ stabilizes no proper subgroup of V. Consequently, Corollary 6.5 implies that $I \cap K[V] \supseteq \omega K[V]$, so $I \supseteq \omega K[V]{\cdot}K[\mathfrak{H}]$, and the result follows. $\square$

In particular, any information on the lattice of ideals of $K[\mathfrak{H}/V]$ carries over immediately to information on the lattice of ideals of $K[\mathfrak{H}]$.

A. Addendum to [OPZ]

This is the promised addendum to [OPZ]. It was added in June, 2001, a bit too late to appear in the published version of that work. However, since then, a modified DVI file for that paper has been available on the author's web page: http://www.math.wisc.edu/~passman. The notation below follows that of the original paper.

Lemma A.1. *Let D be a division ring and let V be a right D-vector space. If* $\operatorname{char} K \neq \operatorname{char} D$*, then any $D^{\bullet}$-stable ideal of $K[V]$ is semiprime.*

Proof. If $\operatorname{char} D = p > 0$, then V is an elementary abelian p-group. In particular, if $\operatorname{char} K \neq p$, then we know that $K[V]$ is a commutative von Neumann regular ring. Hence every ideal of $K[V]$ is semiprime.

On the other hand, if $\operatorname{char} D = 0$, then we must have $\operatorname{char} K = q > 0$ for some prime q. Let I be a $D^{\bullet}$-stable ideal of $K[V]$ and suppose by way of contradiction that $\sqrt{I} > I$. Then we can choose an element $\alpha \in \sqrt{I} \setminus I$ of minimal support size, say $n+1$. Thus $\alpha = k_0x_0 + k_1x_1 + \cdots + k_nx_n$, with $x_0, x_1, \ldots, x_n \in V$ and with $k_0, k_1, \ldots, k_n \in K \setminus 0$. Without loss of generality, we may assume that $k_0 = 1$. Since $\alpha \in \sqrt{I}$ is nilpotent modulo I, we can suppose that $\alpha^{q^s} \in I$ for some integer $s \geq 0$. Of course $\alpha^{q^s} = k_0^{q^s}x_0^{q^s} + k_1^{q^s}x_1^{q^s} + \cdots + k_n^{q^s}x_n^{q^s}$.

Now $\operatorname{char} D = 0$; so $D^{\bullet} \supseteq Q^{\bullet}$, where Q is the field of rational numbers, and hence $1/q^s \in D^{\bullet}$. Thus $d = 1/q^s$ acts on V by taking the unique q^sth root of each element in this uniquely divisible group, and d acts trivially on the field K. Since $\alpha^{q^s} \in I$ and I is d-stable, we see that $\beta = (\alpha^{q^s})^d \in I$ and $\beta = k_0^{q^s}x_0 + k_1^{q^s}x_1 + \cdots + k_n^{q^s}x_n$. Obviously $\operatorname{supp}\alpha = \operatorname{supp}\beta$, and note that $k_0^{q^s} = k_0$ since $k_0 = 1$. Thus $\alpha - \beta$ has support size $\leq n$, and $\alpha - \beta \equiv \alpha \mod I$. In particular, $\alpha - \beta \in \sqrt{I} \setminus I$, contradicting the minimality of n. We conclude that $\sqrt{I} = I$, as required. □

It follows from Lemma A.1 that the semiprime hypotheses in Theorem B and Corollary C of [OPZ] can be eliminated when $\operatorname{char} D \neq \operatorname{char} K$. Finally, we show below that if $\operatorname{char} D = \operatorname{char} K$ and if V is a D-vector space, then there are $D^{\bullet}$-stable ideals of $K[V]$ which cannot be written as a finite product of suitable augmentation ideals.

Example A.2. *Suppose* $\operatorname{char} D = \operatorname{char} K$ *and let V be any right D-vector space of dimension ≥ 2. If B is any proper D-subspace of V, then $I = \omega(B;V) + \omega(V;V)^2$ is a $D^{\bullet}$-stable ideal of $K[V]$ which is neither a finite intersection nor a finite product of augmentation ideals $\omega(A_i;V)$, with each A_i a D-subspace of V.*

Proof. If $\operatorname{char} D = 0$, then V is torsion-free abelian, and if $\operatorname{char} D = p > 0$, then V is an elementary abelian p-group. Thus, since $\operatorname{char} K = \operatorname{char} D$, it follows from [P, Theorems 11.1.10 and 11.1.19] that the dimension subgroups of $K[V]$ satisfy $D_1(K[V]) = V$ and $D_2(K[V]) = 1$.

Now it is obvious that I is a $D^{\bullet}$-stable ideal with $\omega(V;V) \supseteq I \supseteq \omega(V;V)^2$. Note that, for any $b \in B \setminus 1$, we have $b - 1 \in \omega(B;V) \subseteq I$, but $b - 1 \notin \omega(V;V)^2$

since $D_2(K[V]) = 1$. Thus $I > \omega(V;V)^2$. Next, if $I = \omega(V;V)$, then by applying the homomorphism $^{-}\colon K[V] \to K[\overline{V}]$ with $\overline{V} = V/B$, we would obtain $\omega(\overline{V};\overline{V}) = \omega(\overline{V};\overline{V})^2$. But this is a contradiction since $\overline{V}$ is a nonzero D-vector space, and hence $D_1(K[\overline{V}]) = \overline{V} \neq 1 = D_2(K[\overline{V}])$. In other words, $\omega(V;V) > I > \omega(V;V)^2$.

Finally, suppose A is a D-subspace of V satisfying $\omega(A;V) \supseteq I$. Then $\omega(A;V) \supseteq I \supseteq \omega(V;V)^2$ and, by [OPZ, Lemma 1.3(ii)], we know that $\omega(A;V)$ is a $D^{\bullet}$-prime ideal. Thus $\omega(A;V) \supseteq \omega(V;V)$ and $A = V$. It follows that if I is either a finite product or a finite intersection of suitable augmentation ideals $\omega(A_i;V)$, then each A_i is equal to V, so I is a power of $\omega(V;V)$, certainly a contradiction. □

References

[Be] V. V. Belyaev, *Locally finite Chevalley groups* (in Russian), in "Studies in Group Theory", Urals Scientific Centre of the Academy of Sciences of USSR, Sverdlovsk, 1984, pp. 39–50. MR **87d:**20043

[BHPS] K. Bonvallet, B. Hartley, D. S. Passman and M. K. Smith, *Group rings with simple augmentation ideals*, Proc. AMS **56** (1976), 79–82. MR **53:**2996

[BT] A. Borel and J. Tits, *Homomorphismes "abstraits" de groupes algébriques simples*, Ann. Math. **97** (1973), 499–571. MR **47:**5134

[Bo] A. V. Borovik, *Periodic linear groups of odd characteristic*, Soviet Math. Dokl. **26** (1982), 484–486. MR **84d:**20042

[BE] C. J. B. Brookes and D. M. Evans, *Augmentation modules for affine groups*, Math. Proc. Cambridge Philos. Soc. **130** (2001), 287–294. CMP 2001:06

[C] R. W. Carter, *Simple Groups of Lie Type*, Wiley-Interscience, London, 1972. MR **53:**10946

[HS] B. Hartley and G. Shute, *Monomorphisms and direct limits of finite groups of Lie type*, Quart. J. Math. Oxford Ser. (2) **35** (1984), 49–71. MR **85k:**20094

[HZ1] B. Hartley and A. E. Zalesskiĭ, *On simple periodic linear groups – dense subgroups, permutation representations and induced modules*, Israel J. Math. **82** (1993), 299–327. MR **94j:**20046

[HZ2] B. Hartley and A. E. Zalesskiĭ, *Confined subgroups of simple locally finite groups and ideals of their group rings*, J. London Math. Soc. (2) **55** (1997), 210–230. MR **98c:**16031

[J] G. J. Janusz, *Algebraic Number Fields*, 2nd edition, Amer. Math. Soc., Providence, 1996. MR **96j:**11137

[LP] F. Leinen and O. Puglisi, *Ideals in group algebras of simple locally finite groups of* 1*-type*, to appear.

[OPZ] J. M. Osterburg, D. S. Passman, and A. E. Zalesskiĭ, *Invariant ideals of abelian group algebras under the multiplicative action of a field, II*, Proc. Amer. Math. Soc., to appear.

[P] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977. MR **81d:**16001

[PZ] D. S. Passman and A. E. Zalesskiĭ, *Invariant ideals of abelian group algebras and representations of groups of Lie type*. Trans. Amer. Math. Soc. **353** (2001), 2971–2982.

[RS] J. E. Roseblade and P. F. Smith, *A note on hypercentral group rings*, J. London Math. Soc. (2) **13** (1976), 183–190. MR **53:**2997

[S] G. Seitz, *Abstract homomorphisms of algebraic groups*, J. London Math. Soc. (2) **56** (1997), 104–124. MR **99b:**20077

[St] R. Steinberg, *Lectures on Chevalley Groups*, Yale University, New Haven, 1967. MR **57:**6215

[T] S. Thomas, *The classification of simple linear groups*, Archiv der Mathematik **41** (1983), 103–116. MR **85f:**20040b

[Z1] A. E. Zalesskiĭ, *Intersection theorems in group rings* (in Russian), No. 395-74, VINITI, Moscow, 1974.

[Z2] A. E. Zalesskiĭ, *Group rings of inductive limits of alternating groups*, Leningrad Math. J. **2** (1990), 1287–1303. MR **91m:**16026

[Z3] A. E. Zalesskiĭ, *A simplicity condition for the augmentation ideal of the modular group algebra of a locally finite group*, Ukrainian Math. Journal **43** (1991), 1021–1024. MR **93a:**20012

[Z4] A. E. Zalesskiĭ, *Group rings of simple locally finite groups*, in "Proceedings of the Istanbul NATO ASI Conference on Finite and Locally Finite Groups", Kluwer, Dordrecht, 1995, pp. 219–246. MR **96k:**16044

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: passman@math.wisc.edu