Contemporary Mathematics

Polynomial and Inverse Forms

D. S. Passman

Abstract. In a recent paper, this author studied invariant ideals in abelian group algebras under the action of certain infinite, locally finite, quasi-simple groups. While the main result was reasonably definitive, there are nevertheless certain natural extensions that should be considered. One approach to a proof of such extensions is to improve the basic tools that were used in the original work. However, we show here that the two obvious improvements to the polynomial form results fail in general. Specifically, we prove that the final value of a polynomial form $f\colon A \to S$ is not necessarily a subgroup of S. We also show that polynomial forms cannot be extended to "rational function forms" without losing the key properties we require.

1. Introduction

In a recent paper [**P1**], this author studied the ideal structure of group algebras of certain locally finite groups H. Specifically, we assumed that H has a minimal normal abelian subgroup V with $G = H/V$ an infinite quasi-simple group. If I is a nonzero ideal of $K[H]$, then it follows easily that $I \cap K[V]$ is a nonzero ideal of $K[V]$ stable under the action of G. Thus, a first step in this study requires that we understand the G-invariant ideals of $K[V]$, and the main result of [**P1**] is

Theorem 1.1. *Let 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 field $\overline{F}$ also of characteristic p. Assume that G acts nontrivially on V by way of the representation $\phi\colon G \to \mathrm{GL}(V)$, and that V contains no proper G-stable subgroups. If K is a field of characteristic different from p, then the augmentation ideal $\omega K[V]$ is the unique proper G-stable ideal of the group algebra $K[V]$.*

Of course, the assumption that V is a minimal normal subgroup of H guarantees that V contains no proper G-stable subgroups. In particular, V is an irreducible $\overline{F}[G]$-module. But surely this irreducibility condition is a more natural hypothesis for the above result, perhaps under the additional assumption that $\overline{F}$ is the field of character values. In this situation, $K[V]$ may have a number of G-stable ideals. For example, if $V_1, V_2, \ldots, V_k$ are G-stable subgroups of V, then the product

2000 *Mathematics Subject Classification.* Primary 16S34.
Key words and phrases. group rings, invariant ideals, polynomial forms.
Research supported in part by NSA grant 144-LQ65.

$\omega K[V_1]\cdot\omega K[V_2]\cdots\omega K[V_k]\cdot K[V]$ is a G-stable ideal of $K[V]$. We wonder whether ideals of this form are the only possibilities. A natural approach to a proof of this more general proposition is to sharpen the basic tools used in the original work. See [**P2**] for a brief discussion of that argument and also of some earlier results.

Suppose, for example, that $G = \mathrm{SL}_2(F)$ and let $W = F^2$ be the natural 2-dimensional G-module. If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are field automorphisms of F, then G acts on the tensor product module $V = W^{\sigma_1} \otimes W^{\sigma_2} \otimes \cdots \otimes W^{\sigma_n}$ and a maximal torus T of G acts on a particular line L of V with eigenfunction $\theta\colon x \mapsto x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n}$. Certainly, θ is an endomorphism of the multiplicative group $F^\bullet$. Next we let $\lambda\colon F^+ \to S$ be an additive group homomorphism from F^+ to the finite abelian group S and we form the composite map $\lambda\circ\theta\colon F \to S$ given by $\lambda\circ\theta(x) = \lambda(x^{\sigma_1}x^{\sigma_2}\cdots x^{\sigma_n})$. What we have here is a polynomial form on F^+, and the study of such forms is a key ingredient in the proof of Theorem 1.1.

To be precise, let $\mathfrak{Z}$ be a ring, let A be an infinite left $\mathfrak{Z}$-module and let S be a finite abelian group. Then the *polynomial forms* on A are functions $f\colon A \to S$ that satisfy the following inductive conditions as given in [**P1**]. By definition, a polynomial form of degree 0 is the zero function, and for $n \geq 1$, we say that f is a polynomial form of degree $\leq n$ if and only if:

i. $f(a) = 0$ implies that $f(\mathfrak{Z}a) = 0$.
ii. For each $a \in A$, the function $\tilde{f}_a(x) = f(a+x) - f(a) - f(x)$ 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. The following is part of [**P1**, Lemma 2.2].

LEMMA 1.2. *Let $\mathfrak{Z}$, A and S be as above.*

i. *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 $f(A) = 0$.*
ii. *Let R be an infinite ring, fix $r_0, r_1, \ldots, r_n \in R$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be $n \geq 1$ endomorphisms of R. Next, let $\mathfrak{Z}$ be a central subring of R that is stable under each σ_i, and let $A = R^+$ 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 $f(x) = \lambda(r_0x^{\sigma_1}r_1x^{\sigma_2}r_2\cdots r_{n-1}x^{\sigma_n}r_n)$ is a polynomial form on A of degree $\leq n$.*

The key property of polynomial forms that was used in the proof of Theorem 1.1 is [**P1**, Proposition 2.3], namely

PROPOSITION 1.3. *Let $\mathfrak{Z}$, A and S be as above and let $f\colon A \to S$ be a finite sum of polynomial forms. If B is any infinite $\mathfrak{Z}$-submodule of A, then there exists an infinite submodule C of B with $f(C) = 0$.*

In other words, any finite sum of polynomial forms is *eventually null*. 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 it the *final value* of f. In view of [**P1**, Example 2.6 and Proposition 3.4(ii)], paper [**P1**] asked whether the final value of a polynomial form f is necessarily always a subgroup of S. This is certainly true if

$\deg f \leq 1$ and the following result of [**O**] shows that it is true for polynomial forms of degree ≤ 2.

LEMMA 1.4. *Let $f\colon A \to S$ be a polynomial form.*

i. *If, for all $a \in A$, $\tilde{f}_a = f(a+x) - f(a) - f(x)$ vanishes on a submodule of A of finite index, then the final value of f is a subgroup of S.*
ii. *If $\deg f \leq 2$, then the final value of f is a subgroup of S.*

PROOF. (i) Let $f(B) \subseteq S$ be the final value of f. We need to show that $f(B)$ is closed under addition. To this end, let $\alpha, \beta \in f(B)$ and choose $a \in B$ with $f(a) = \alpha$. By assumption, $\tilde{f}_a(x) = f(a+x) - f(a) - f(x)$ vanishes on some submodule C of finite index in A. Thus $\tilde{f}_a$ vanishes on $B \cap C$. But $|A : B \cap C| < \infty$, so $f(B \cap C) = f(B)$ and we can choose $b \in B \cap C$ with $f(b) = \beta$. Then $0 = \tilde{f}_a(b) = f(a+b) - f(a) - f(b)$, so $f(a+b) = f(a) + f(b) = \alpha + \beta$. Since $a + b \in B$, we conclude that $\alpha + \beta \in f(B)$, as required.

(ii) If $\deg f \leq 2$, then $\tilde{f}_a(x)$ is a finite sum of polynomial forms of degree ≤ 1. Since each such form of degree ≤ 1 vanishes on a submodule of A of finite index, we see that $\tilde{f}_a(x)$ vanishes on a suitable submodule of finite index and part (i) above yields the result. □

In this note, we show by example that final values need not be subgroups in general. Now let us return to the group $\mathrm{SL}_2(F)$ discussed above and observe that the other eigenfunctions of the maximal torus T are given by $x \mapsto x^{\pm\sigma_1} x^{\pm\sigma_2} \cdots x^{\pm\sigma_n}$. Once negative exponents are present, these eigenfunctions no longer yield polynomial forms but rather maps that we might be tempted to call *rational function forms*. Whatever the formal definition might be, there is a natural special case that is certainly of interest. Namely, let F be an infinite field and let $\mathfrak{Z}$ be a finite subfield. Suppose A is an infinite $\mathfrak{Z}$-submodule of F and let $\lambda\colon A \to S$ be a homomorphism to the finite abelian group S with $\ker\lambda$ a $\mathfrak{Z}$-submodule of A. Then we call the composite map $f\colon A \setminus 0 \to S$ given by $x \mapsto \lambda(x^{-1})$ an *inverse form* on A, and a natural question is whether such forms are necessarily eventually null. In this note, we show by example that this property also fails in general.

The author would like to thank Prof. J. M. Osterburg for rekindling his interest in the final value problem and for suggesting the clever last example discussed in the next section.

2. The Final Value

All of the examples in this section take $\mathfrak{Z}$ to be 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. Indeed, we have the following generalization of [**P1**, Example 2.4] with essentially the same proof.

EXAMPLE 2.1. *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 and if S is a finite elementary abelian p-group, then there exists a polynomial form $f\colon A \to S$ of degree ≤ 2 which is onto when restricted to 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 K-vector space, so there exists a subspace V of A of codimension 1 with $V \supseteq C$. Furthermore, since A/V is an infinite elementary abelian p-group, there exists a group epimorphism $\lambda\colon A \to S$ with kernel $L \supseteq V \supseteq C$. Define $f\colon A \to S$ by $f(x) = \lambda(x^2)$ so that f is a polynomial form of degree ≤ 2 by Lemma 1.2(ii). Furthermore, since $C \subseteq L$, it is clear that $f(C) = 0$. If B is a subgroup of A of finite index, our goal is to show that $f(B) = S$.

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 $\tilde{f}_u\colon A \to S$ given by $\tilde{f}_u(x) = f(u + x) - f(u) - f(x) = \lambda(2ux)$ 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 $f(B') \subseteq f(B)$. To this end, let $b' = u + d$ be an arbitrary element of B' with $u \in U$ and $d \in D$. Then $f(b') = f(u + d) = f(u) + f(d) + \tilde{f}_u(d) = f(d)$ since $f(u) \in f(C) = 0$ and since $d \in D_u$ implies that $\tilde{f}_u(d) = 0$. But $D \subseteq B$, so $f(b') = f(d) \in f(B)$ and consequently $f(B') \subseteq f(B)$, as claimed. Thus, it suffices to show that $f(B') = S$. Replacing B by B' if necessary, we may now suppose that $B \supseteq C$.

Since $KB \supseteq B$, the quotient A/KB is a finite vector space over the infinite field K. Thus $A/KB = 0$ and $A = KB$. In particular, there exists $b_0 \in B$ with $b_0 \notin V$ and, since V has codimension 1 in A, it follows that $A = V + Kb_0 = L + Kb_0$. Hence $S = \lambda(A) = \lambda(Kb_0) = 2\lambda(Kb_0)$ since $p \neq 2$. Finally, if $c \in C = K^+$, then

$$f(c + b_0) = f(c) + f(b_0) + 2\lambda(cb_0) = f(b_0) + 2\lambda(cb_0)$$

and consequently

$$f(C + b_0) = f(b_0) + 2\lambda(Cb_0) = f(b_0) + S = S.$$

But $B \supseteq C$, so $B \supseteq C + b_0$ and we conclude that $f(B) = S$, as required.

Note that, when $p = 2$, the map $f(x) = \lambda(x^2)$ is a group homomorphism which has a kernel $\overline{B}$ of finite index in A. In particular, $f(\overline{B}) \neq S$ if S is chosen to be nonzero.

(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 $C = K^+$, choose $V \supseteq C$ to be a K-subspace of codimension 1 in A and let $\lambda\colon A \to S$ be a group epimorphism with kernel $L \supseteq V$. Now 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 1.2(ii). If B is a subgroup of A of finite index, our goal is to show that $f(B) = S$. As above, we can assume that $B \supseteq C$ and that there exists $b_0 \in B$ with $\lambda(Cb_0) = S$.

Let $c \in C$ and observe that

$$\begin{aligned}(c + b_0)^\sigma (c + b_0)^{\sigma^{-1}} &= c^\sigma c^{\sigma^{-1}} + b_0^\sigma b_0^{\sigma^{-1}} + c(b_0^\sigma + b_0^{\sigma^{-1}}) \\ &= c^\sigma c^{\sigma^{-1}} + b_0^\sigma b_0^{\sigma^{-1}} + c(b_0 + b_0^\sigma + b_0^{\sigma^{-1}}) - cb_0\end{aligned}$$

since c is fixed by σ. Furthermore, $c^\sigma c^{\sigma^{-1}} = c^2 \in K \subseteq L$ and, since σ has order 3, we also have $c(b_0 + b_0^\sigma + b_0^{\sigma^{-1}}) \in K \subseteq L$. Thus, by applying λ to the above displayed equation, we obtain $f(c + b_0) = f(b_0) - \lambda(cb_0)$ and hence

$$f(C + b_0) = f(b_0) - \lambda(Cb_0) = f(b_0) - S = S.$$

Since $B \supseteq C + b_0$, we conclude that $f(B) = S$ and the result follows. □

Next, we need an extension of [**P1**, Lemma 2.5]. Here we assume that S is the additive group of a finite field E and we use the multiplication in E to combine polynomial forms. $\mathfrak{Z}$ can be any ring.

LEMMA 2.2. *Let A be an infinite $\mathfrak{Z}$-module, let E be a finite field of characteristic $p > 0$, and write $S = E^+$. Let $f\colon A \to S$ be a polynomial form of degree $\leq n$.*

i. *If $c \in E$, then the product $cf\colon A \to S$ is a polynomial form of degree $\leq n$.*
ii. *If $g\colon A \to S$ is a polynomial form of degree $\leq m$, then the product of the two forms $fg\colon A \to S$ is a polynomial form of degree $\leq n + m$.*
iii. *The pth power $f^p\colon A \to S$ is a polynomial form of degree $\leq n$.*

PROOF. (i) We proceed by induction on n. Since the case $n = 0$ is trivial, we can assume that $n \geq 1$. We can also assume that $c \neq 0$. If $cf(a) = 0$, then $f(a) = 0$ since E is a field. Thus $f(\mathfrak{Z}a) = 0$ and hence $cf(\mathfrak{Z}a) = 0$. Again, if $a \in A$, then $f(a+x) - f(a) - f(x) = \tilde{f}_a(x)$ is a finite sum of polynomial forms of degree $\leq n-1$. Multiplying this equation by c and applying induction clearly yields the result.

(ii) Here we proceed by induction on $n + m$ and we can clearly assume that $n, m \geq 1$. If $fg(a) = f(a)g(a) = 0$, then $f(a) = 0$ or $g(a) = 0$ and hence either $f(\mathfrak{Z}a) = 0$ or $g(\mathfrak{Z}a) = 0$. In either case, this yields $fg(\mathfrak{Z}a) = 0$. Now let $a \in A$ be arbitrary and write $f(a+x) - f(a) - f(x) = \tilde{f}_a(x)$ and $g(a+x) - g(a) - g(x) = \tilde{g}_a(x)$, where $\tilde{f}_a(x)$ is a sum of polynomial forms of degree $\leq n - 1$ and $\tilde{g}_a(x)$ is a sum of polynomial forms of degree $\leq m - 1$. Then

$$\begin{aligned} fg(a + x) - fg(a) - fg(x) = {} & f(x)g(a) + f(a)g(x) \\ & + \tilde{f}_a(x)g(a) + f(a)\tilde{g}_a(x) \\ & + f(x)\tilde{g}_a(x) + \tilde{f}_a(x)g(x) + \tilde{f}_a(x)\tilde{g}_a(x). \end{aligned}$$

Since $n, m \geq 1$, it follows from part (i) that the first four terms of the above right-hand side are sums of polynomial forms of degree $\leq n + m - 1$. By induction, the remaining three terms are sums of polynomial forms of degree $\leq n + m - 1$. With this, we conclude that fg is a polynomial form of degree $\leq n + m$.

(iii) Since $\tilde{f}_a(x) = f(a + x) - f(a) - f(x)$, we have

$$(\tilde{f}_a)^p(x) = f^p(a + x) - f^p(a) - f^p(x)$$

and hence $(\widetilde{f^p})_a = (\tilde{f}_a)^p$. But we know that $\tilde{f}_a$ is a finite sum of polynomial forms of degree $\leq n - 1$, so the linearity of the p-power map and induction imply that $(\widetilde{f^p})_a$ is also a finite sum of polynomial forms of degree $\leq n - 1$. Thus f^p is indeed a polynomial form of degree $\leq n$. □

By combining the previous two results, we can now easily construct a counterexample of degree ≤ 4 to the final value conjecture.

EXAMPLE 2.3. *Let A and S be elementary abelian p-groups with A infinite and with S finite.*

i. *If $p > 2$ and $|S| = p^n > 1$, then there exists a polynomial form $f\colon A \to S$ of degree ≤ 4 whose final value is not a subgroup of S.*
ii. *If $p = 2$ and $|S| = 2^{2n}$ with $n \geq 2$, then there exists a polynomial form $f\colon A \to S$ of degree ≤ 4 whose final value is not a subgroup of S.*

PROOF. (i) There exists a field F of characteristic p such that $A \cong F^+$ and such that F has an infinite proper subfield. By Example 2.1(i), there exists a polynomial form $g\colon A \to S$ of degree ≤ 2 which is onto when restricted to any subgroup of A of finite index. Now let $E = \mathrm{GF}(p^n)$ so that $S \cong E^+$ and, using the multiplication in E, define $f = g^2\colon A \to S$. By Lemma 2.2(ii), f is a polynomial form of degree ≤ 4. Now if B is any subgroup of A of finite index, then $g(B) = S$ implies that $f(B) = \{s^2 \mid s \in S\} = T$. In particular, T is the final value of f and, since $|T| = (p^n + 1)/2 > p^{n-1}$, we see that T is not a subgroup of S.

(ii) The argument here is similar. Let F be a field of characteristic 2 such that $A \cong F^+$ and such that F admits an automorphism of order 3. By Example 2.1(ii), there exists a polynomial form $g\colon A \to S$ of degree ≤ 2 which is onto when restricted to any subgroup of A of finite index. Now let $E = \mathrm{GF}(2^{2n})$ so that $S \cong E^+$ and, using the multiplication in E, define $f = g^3\colon A \to S$. By Lemma 2.2(ii)(iii), the map $f = g \cdot g^2$ is a polynomial form of degree ≤ 4. Now if B is any subgroup of A of finite index, then $g(B) = S$ implies that $f(B) = \{s^3 \mid s \in S\} = T$. In particular, T is the final value of f and, since $|T| = (2^{2n} + 2)/3$ is not a power of 2 when $n \geq 2$, it follows that T is not a subgroup of S. □

The following construction was suggested by J. M. Osterburg. It can be used as a replacement for Example 2.1 in the preceding work.

EXAMPLE 2.4. *Let p be a prime and let $\mathrm{GF}(p)$ denote the field with p elements.*

i. *Suppose $p > 2$ and let k be a fixed integer that satisfies $2 \leq k < p$. Next, let $A = \bigoplus_i \mathrm{GF}(p)_i$ be an infinite direct sum of copies of $\mathrm{GF}(p)$ and define $f\colon A \to \mathrm{GF}(p)$ by $\bigoplus_i a_i \mapsto \sum_i a_i^k$. Then f is a polynomial form of degree $\leq k$ and f is onto when restricted to any subgroup of A of finite index.*
ii. *Suppose $A = \bigoplus_i \mathrm{GF}(4)_i$ is an infinite direct sum of copies of $\mathrm{GF}(4)$ and define $f\colon A \to \mathrm{GF}(2)$ by $\bigoplus_i a_i \mapsto \sum_i a_i^3$. Then f is a polynomial form of degree 2 and f is onto when restricted to any finite index subgroup of A.*

PROOF. (i) A simple inductive argument, which we skip, proves that f is a polynomial form of degree $\leq k$.

We show now that f cannot vanish on any subgroup of A of finite index. To this end, suppose $f(B) = 0$ with $|A : B| = p^m < \infty$. If k is even, then we have the following simple argument. For each i, let η_i denote the element of A having a 1 in the ith coordinate and zeros elsewhere. Since $|A : B| < \infty$ and there are infinitely many η_is, there exist $i \neq j$ with $\eta_i \equiv \eta_j \bmod B$. Thus $\eta_i - \eta_j \in B$, but $0 \neq 2 = f(\eta_i - \eta_j) \in f(B)$, contradiction.

For general k, choose $n > 2m$ and let $V = \bigoplus_{i=1}^n \mathrm{GF}(p)_i$ be the $\mathrm{GF}(p)$-subspace of A of dimension n consisting of the first n summands. Then the restriction of f to V vanishes on $B \cap V$, a subspace of codimension $\leq m$. Thus $\dim(B \cap V) \geq n - m$. Now if $\alpha = \bigoplus_{i=1}^n a_i$ and $\beta = \bigoplus_{i=1}^n b_i$ belong to $B \cap V$, then $f(\alpha + t\beta) = 0$ for all

$t = 0, 1, \dots, p-1$ yields

$$\sum_i a_i^k + t\binom{k}{1}\sum_i a_i^{k-1}b_i + \cdots + t^{k-1}\binom{k}{k-1}\sum_i a_i b_i^{k-1} + t^k \sum_i b_i^k = 0.$$

Thus, since $k \le p-1$ and since a Vandermonde matrix with distinct parameters is nonsingular, we have $\sum_{i=1}^n a_i b_i^{k-1} = 0$. In particular, with respect to the usual dot product, we see that the vector $\beta^{k-1} = \bigoplus_{i=1}^n b_i^{k-1}$ is perpendicular to all members of $B \cap V$. In other words, $\{\beta^{k-1} \mid \beta \in B \cap V\} \subseteq (B \cap V)^\perp$, a subspace of V of dimension $\le n-(n-m) = m$. On the other hand, if we choose a basis for $B \cap V$ that is in echelon form then, since $k \ge 2$, the $(k-1)$st powers of these basis vectors are also in echelon form and hence are linearly independent. It follows that the subspace of V spanned by $\{\beta^{k-1} \mid \beta \in B \cap V\}$ has dimension $\ge \dim(B \cap V) \ge n - m$. Since this subspace is contained in $(B \cap V)^\perp$, we conclude that $m \ge \dim(B \cap V)^\perp \ge n - m$, contradicting the fact that we chose $n > 2m$.

We conclude therefore that f does not vanish on any subgroup of A of finite index. In particular, the final value of f is nonzero. But if $\alpha = \bigoplus_i a_i$ is an arbitrary element of A, then $\tilde{f}_\alpha(x) = f(\alpha + x) - f(\alpha) - f(x)$ vanishes on the partial direct sum $\bigoplus_j \mathrm{GF}(p)_j$ consisting of those coordinates j with $a_j = 0$. In other words, $\tilde{f}_\alpha$ vanishes on a subgroup of A of finite index. Lemma 1.4(i) now implies that the final value of f is a subgroup of $\mathrm{GF}(p)$ and, since it is nonzero, this final value must be precisely $\mathrm{GF}(p)$.

(ii) The argument here is similar to the general case above, but slightly more complicated, and we just sketch the key ideas. First observe that if $a \in \mathrm{GF}(4)$, then $a^3 = 0$ or 1 and hence $a^3 \in \mathrm{GF}(2)$. Thus f does indeed map A to $\mathrm{GF}(2)$. Furthermore, if $\alpha = \bigoplus_i a_i$ and if $x = \bigoplus_i x_i$, then

$$\tilde{f}_\alpha(x) = \sum_i (a_i + x_i)^3 - \sum_i a_i^3 - \sum_i x_i^3 = \sum_i a_i^2 x_i + \sum_i a_i x_i^2$$

and this is a linear function of x. Thus f is a polynomial form of degree ≤ 2. Indeed, $\deg f = 2$ since $\tilde{f}_\alpha$ is not always 0.

Again, we show that f does not vanish on any subgroup of A of finite index. To this end, suppose $f(B) = 0$ with $|A : B| = 2^m$. Choose $n > 2m$, let $V = \bigoplus_{i=1}^n \mathrm{GF}(4)_i$ and let $W = \bigoplus_{i=1}^n \mathrm{GF}(2)_i$. Then, as vector spaces over $\mathrm{GF}(2)$, we have $\dim W = n$ and $\dim V/W = n$. From the above, if $\alpha = \bigoplus_{i=1}^n a_i$ and $\beta = \bigoplus_{i=1}^n b_i$ are in $B \cap V$, then $\sum_{i=1}^n (a_i^2 b_i + a_i b_i^2) = 0$. Now if $\alpha \in B \cap W$, then $a_i \in \mathrm{GF}(2)$, so $a_i^2 = a_i$ and the above yields

$$0 = \sum_{i=1}^n a_i(b_i + b_i^2) = \sum_{i=1}^n a_i \operatorname{tr}(b_i),$$

where $\operatorname{tr}\colon \mathrm{GF}(4) \to \mathrm{GF}(2)$ is the Galois trace.

Note that tr is a linear map and that, in our case, it vanishes on $\mathrm{GF}(2)$. Thus the above gives rise to a map $W \times (V/W) \to \mathrm{GF}(2)$ and this is easily seen to be a nondegenerate bilinear form. Since $(B \cap W) \times [(B \cap V) + W]/W$ maps to 0, we see that $\dim(B \cap W) + \dim[(B \cap V) + W]/W \le n$. But each of the dimensions $\dim(B \cap W)$ and $\dim[(B \cap V) + W]/W$ is at least equal to $n - m$, so $2(n-m) \le n$ and $n \le 2m$, a contradiction. Thus f does not vanish on any subgroup of A of finite index and, since $S = \mathrm{GF}(2)$, it is clear that the final value of f is $\mathrm{GF}(2)$. $\square$

Of course, the above construction only yields final values equal to $\mathrm{GF}(p)$, but it is a simple matter to obtain larger $\mathrm{GF}(p)$-vector spaces. Indeed, suppose S is a $\mathrm{GF}(p)$-vector space with basis $s_1, s_2, \ldots, s_t$ and let f be as above. Then we define $g\colon A_1 \oplus A_2 \oplus \cdots \oplus A_t \to S$, where the domain $\overline{A}$ is the direct sum of t copies of A, by $g\colon \alpha_1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_t \mapsto \sum_{i=1}^t f(\alpha_i)s_i$. Clearly g is a polynomial form of the same degree as that of f. Furthermore, if $\overline{B}$ is a subgroup of $\overline{A}$ of finite index and if we set $B_i = \overline{B} \cap A_i$. then $|A_i : B_i| < \infty$ and $\overline{B} \supseteq B_1 \oplus B_2 \oplus \cdots \oplus B_t$. Thus $f(\overline{B}) \supseteq \sum_{i=1}^t f(B_i)s_i = \sum_{i=1}^t \mathrm{GF}(p)s_i = S$ and S is the final value of g.

3. Inverse Forms

Let K be an infinite field of characteristic $p > 0$ and let $\mathfrak{Z}$ be a finite subfield. Suppose A is an infinite $\mathfrak{Z}$-submodule of K and let $\lambda\colon K^+ \to S$ be a group homomorphism to the finite group S with $\ker\lambda$ being a $\mathfrak{Z}$-submodule of K. Then we recall that the function $f\colon A\setminus 0 \to S$ given by $x \mapsto \lambda(x^{-1})$ is called an inverse form on A. We first show that there exist inverse forms which are not eventually null. Indeed, there exist such forms which never take on the value 0.

Example 3.1. *If K is an infinite field of characteristic $p > 0$, then there exists an infinite abelian subgroup A of K^+ and a linear functional $\lambda\colon K^+ \to \mathrm{GF}(p)$, such that $\lambda(a^{-1}) \neq 0$ for all $0 \neq a \in A$. In particular, the inverse form $f\colon A\setminus 0 \to \mathrm{GF}(p)$ given by $f(x) = \lambda(x^{-1})$ does not vanish on any nonzero subgroup of A.*

Proof. Note that K^+ is an infinite elementary abelian p-group and that every subgroup is a $\mathrm{GF}(p)$-subspace. We show by induction on $n \geq 1$ that K^+ has three increasing sequences of finite subgroups $\{A_n\}$, $\{B_n\}$ and $\{C_n\}$ with

(1) $|A_n| = p^n$,
(2) $B_n \supseteq C_n$ and $|B_n : C_n| = p$, and
(3) $a^{-1} \in B_n \setminus C_n$ for all $0 \neq a \in A_n$.

For $n = 1$, we can clearly take $A_1 = B_1 = \mathrm{GF}(p)$ and $C_1 = 0$.

Now suppose that A_n, B_n and C_n are given and choose any fixed $\beta \in B_n \setminus C_n$. If $x \in K \setminus A_n$ and $a \in A_n$, define $x(a) = (x - a)^{-1} - \beta$, and observe that any dependence relation of the form

$$b + \sum_{a\in A_n} \gamma(a)x(a) = 0$$

with $b \in B_n$ and $\gamma(a) \in \mathrm{GF}(p)$ gives rise to a polynomial equation satisfied by x once we clear denominators by multiplying by $\prod_{a\in A_n}(x - a)$. Indeed, this polynomial evaluated at any $a \in A_n$ is equal to $\gamma(a)$, and hence if some $\gamma(a)$ is nonzero then the polynomial is nonzero. As a consequence, we see that there are only finitely many $x \in K \setminus A_n$ that satisfy any such nontrivial relation. Thus, since there are only finitely many choices for $b \in B_n$ and for the various $\gamma(a) \in \mathrm{GF}(p)$ and since K is infinite, we see that there exists an element $x \in K \setminus A_n$ such that if

$$b + \sum_{a\in A_n} \gamma(a)x(a) = 0,$$

then $\gamma(a) = 0$ for all $a \in A_n$ and hence $b = 0$.

For this x, let

$$\begin{aligned} A_{n+1} &= A_n + \mathrm{GF}(p)x, \\ B_{n+1} &= B_n + \sum_{a\in A_n} \mathrm{GF}(p)x(a), \text{ and} \\ C_{n+1} &= C_n + \sum_{a\in A_n} \mathrm{GF}(p)x(a). \end{aligned}$$

Certainly, $|A_{n+1}| = p{\cdot}|A_n| = p^{n+1}$, $B_{n+1} \supseteq C_{n+1}$ and $|B_{n+1} : C_{n+1}| = p$ since linear independence implies that $C_{n+1} \cap B_n = C_n$. Of course, if $0 \neq a \in A_n$, then $a^{-1} \in B_n \setminus C_n \subseteq B_{n+1} \setminus C_{n+1}$. Furthermore, if $a \in A_n$, then $(x-a)^{-1} = x(a)+\beta \in B_{n+1}\setminus C_{n+1}$ since $x(a) \in C_{n+1}$ and $\beta \in B_n \setminus C_n \subseteq B_{n+1}\setminus C_{n+1}$. Finally, if $\alpha \in A_{n+1} \setminus A_n$, then $\alpha = \gamma x - a$ for some $0 \neq \gamma \in \mathrm{GF}(p)$ and $a \in A_n$. Thus

$$\alpha^{-1} = \frac{1}{\gamma x - a} = \gamma^{-1}\frac{1}{x - \gamma^{-1}a} \in B_{n+1} \setminus C_{n+1}$$

and the induction step is proved.

We can now set $A = \bigcup_n A_n$, $B = \bigcup_n B_n$ and $C = \bigcup_n C_n$. Then these are infinite subgroups of K^+ clearly satisfying $|B : C| = p$ and $a^{-1} \in B \setminus C$ for all $0 \neq a \in A$. If $\lambda\colon K^+ \to \mathrm{GF}(p)$ is any extension of the functional $B \to B/C \cong \mathrm{GF}(p)^+$, then $\lambda(a^{-1}) \neq 0$ for all $0 \neq a \in A$, so λ and A have the required properties. □

An alternate more concrete construction of such an example is given below. Here, however, we require K to be a rational function field over a finite field. For simplicity, we write $A^{-1} = \{a^{-1} \mid a \in A \setminus 0\}$.

Example 3.2. *Let $K = F(x)$ be the rational function field in the indeterminate x over the finite field F. Then there exists an infinite dimensional F-subspace A of K^+ and a linear functional $\lambda\colon K^+ \to F$, such that $\lambda(a^{-1}) \neq 0$ for all $0 \neq a \in A$. In particular, the inverse form $f\colon A \setminus 0 \to F$ given by $f(x) = \lambda(x^{-1})$ does not vanish on any nonzero subgroup of A. Furthermore, we can assume that $1 \in A$ and that $A^p \subseteq A$ if $\operatorname{char} F = p > 2$. On the other hand, if $\operatorname{char} F = 2$, then we can at least assume that $A^4 \subseteq A$.*

Proof. Embed $K = F(x)$ in E, the field of Laurent series in x over F. Let $\lambda\colon E \to F$ be given by $\lambda\colon \sum_i a_i x^i \mapsto a_0$ so that $L' = \ker_E \lambda$ has codimension 1 in E as an F-subspace. Hence $L = \ker_K \lambda = L' \cap K$ has F-codimension 1 in K.

Let $q > 2$ be an integer and let A be the F-subspace of $F[x] \subseteq F(x)$ spanned by the polynomials

$$1, x(1-x), x^q(1-x^q), x^{q^2}(1-x^{q^2}), \ldots, x^{q^n}(1-x^{q^n}), \ldots.$$

Since these polynomials have distinct degrees, they are linearly independent and hence $\dim_F A = \infty$. Let $0 \neq \alpha \in A$ and write α as the finite sum

$$\alpha = a + \sum_{i=0}^{\infty} b_i x^{q^i}(1-x^{q^i}),$$

with $a, b_i \in F$. We show that $\alpha^{-1} \notin L$ by computing α^{-1} in E and showing that $\alpha^{-1} \notin L' = \ker\lambda$.

Suppose first that $a \neq 0$. Then $\alpha = a(1 - x \cdot p(x))$ for some polynomial $p(x) \in F[x]$ and hence

$$\alpha^{-1} = a^{-1}(1 - x \cdot p(x))^{-1} = a^{-1} \sum_{k=0}^{\infty} x^k \cdot p(x)^k = a^{-1}(1 + x \cdot s(x))$$

for some power series $s(x)$. Thus $\lambda(\alpha^{-1}) = a^{-1} \neq 0$ and $\alpha^{-1} \notin L'$.

Now suppose that $a = 0$. Then, for some integer $n \geq 0$, we can write

$$\alpha = f x^{q^n}(1 - x^{q^n}) + g x^{q^{n+1}}(1 - x^{q^{n+1}}) + \cdots$$

with $0 \neq f \in F$. Since $1 - x^{q^n}$ divides $1 - x^{q^m}$ for all $m \geq n$, we have

$$\alpha = f x^{q^n}(1 - x^{q^n})(1 - h x^{q^{n+1} - q^n} + \text{larger degree terms}).$$

Thus, using "ldt" to denote "larger degree terms", we obtain

$$\begin{aligned} \alpha^{-1} &= f^{-1} x^{-q^n}(1 - x^{q^n})^{-1}(1 - h x^{q^{n+1} - q^n} + \text{ldt})^{-1} \\ &= f^{-1} x^{-q^n}(1 + x^{q^n} + \text{ldt})(1 + h x^{q^{n+1} - q^n} + \text{ldt}). \end{aligned}$$

But $q > 2$, so $q^{n+1} - q^n > q^n$ and it follows that

$$\alpha^{-1} = f^{-1} x^{-q^n} + f^{-1} x^0 + \text{ldt}.$$

In particular, $\lambda(\alpha^{-1}) = f^{-1} \neq 0$ and again $\alpha^{-1} \notin L'$.

Finally, if $\operatorname{char} F = p > 2$, we can take $q = p$ and see that $A^p \subseteq A$. On the other hand, if $\operatorname{char} F = 2$, we can at least take $q = 4$ and have $A^4 \subseteq A$. □

Now we turn this problem around and indicate a few techniques that can be used to prove that $A^{-1} \cap L = A^{-1} \cap \ker \lambda \neq \emptyset$ in at least some situations. To start with, we have

LEMMA 3.3. *Suppose K is a field containing the finite subfield F, and let L and A be F-subspaces of K with $\dim_F K/L = 1$. If there exists an element $t \notin F$ with $1, t, t^2 \in A$, then $A^{-1} \cap L \neq \emptyset$.*

PROOF. If $a \in F$, then $a + t \neq 0$ and hence we can consider the elements $(a + t)^{-1} \in K$. If these elements are in different cosets of L then, since we have $|F|$ such elements and $|F|$ such cosets, it follows that there exists $a \in F$ with $(a + t)^{-1} \equiv 0 \mod L$. By assumption, $(a + t)^{-1} \in A^{-1} \cap L$.

On the other hand, if these elements are not in different cosets, then there exist $a \neq b$ in F with $(a + t)^{-1} \equiv (b + t)^{-1} \mod L$. Thus

$$\frac{a - b}{(a + t)(b + t)} = \frac{1}{b + t} - \frac{1}{a + t} \in L.$$

But $(a + t)(b + t)/(a - b) \in A$, since $1, t, t^2 \in A$ and since A is an F-subspace of K. Thus, again we have $A^{-1} \cap L \neq \emptyset$. □

Next, we need

LEMMA 3.4. *For each integer $n \geq 1$, there exist distinct nonconstant monic integer polynomials $f_1(x), f_2(x), \ldots, f_n(x)$ such that*

i. *$f_i(x) \mid f_{i+1}$ for all $1 \leq i < n$,*
ii. *$(f_i(x) - f_j(x)) \mid f_i(x) f_j(x)$ for all $1 \leq j < i \leq n$, and*
iii. *$\deg f_n(x) < 2^{n!}$.*

PROOF. We proceed by induction on n, the result being trivial for $n = 1$ by choosing the unique polynomial to equal x. Now suppose the result holds for $n \geq 1$ and let $f_1(x), f_2(x), \ldots, f_n(x)$ satisfy the above conditions. We then define the distinct monic polynomials $g_0(x), g_1(x), \ldots, g_n(x)$ by $g_0(x) = \prod_{k=1}^{n}(f_k(x) - 1)$ and $g_i(x) = g_0(x)f_i(x)$ for all $1 \leq i \leq n$. Then it is clear that $g_i(x) \mid g_{i+1}(x)$ for all $0 \leq i < n$ and that $(g_i(x) - g_j(x)) \mid g_i(x)g_j(x)$ for all $1 \leq j < i \leq n$. Furthermore, for $i \geq 1$, the definition of $g_0(x)$ implies that $(g_i(x) - g_0(x)) = g_0(x)(f_i(x) - 1)$ divides $g_0(x)g_i(x) = g_0(x)^2 f_i(x)$. Finally, since $\deg f_i(x) \leq \deg f_n(x) < 2^{n!}$, we see that $\deg g_0(x) \leq 2^{n! \cdot n}$ and hence

$$\deg g_n(x) = \deg g_0(x) + \deg f_n(x) < 2^{n! \cdot n} + 2^{n!} \leq 2^{n! \cdot n + n!} = 2^{(n+1)!},$$

as required. Induction now yields the result. □

Finally, we extend Lemma 3.3 to more general subgroups of finite index by assuming that A contains a large number of consecutive powers of a given element. Specifically, we prove

LEMMA 3.5. *Let K be a field of characteristic $p > 0$ and let L be an additive subgroup of finite index $|K : L| < n$. Furthermore, let A be an additive subgroup of K and suppose that either*

i. *there exists an element $t \in K$ such that $t, t^2, \ldots, t^{n!} \in A$ and these elements are linearly independent over* $\mathrm{GF}(p)$*, or*
ii. *$|K| = \infty$ and $|K : A| < \infty$.*

Then $A^{-1} \cap L \neq \emptyset$.

PROOF. (i) Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the monic integer polynomials given by the preceding lemma and view these as belonging to the polynomial ring $\mathrm{GF}(p)[x]$. Since $\deg f_i(x) < 2^{n!}$, it follows that each $t \cdot f_i(t)$ is a nonzero element of K. Thus we can take their inverses and obtain n elements $t^{-1} \cdot f_i(t)^{-1} \in K$. But $|K : L| < n$, by assumption, so there must exist $i > j$ with $t^{-1} \cdot f_i(t)^{-1} \equiv t^{-1} \cdot f_j(t)^{-1} \mod L$. In particular,

$$\frac{f_i(t) - f_j(t)}{t \cdot f_i(t) f_j(t)} = \frac{1}{t \cdot f_j(t)} - \frac{1}{t \cdot f_i(t)} \in L.$$

Now we know that $(f_i(x) - f_j(x)) \mid f_i(x)f_j(x)$ and that $\deg f_i(x) > \deg f_j(x)$. Thus $\deg(f_i(x) - f_j(x)) = \deg f_i(x)$ and it follows that $f_i(x)f_j(x) = (f_i(x) - f_j(x)) \cdot g(x)$ with $\deg g(x) = \deg f_j(x) < 2^{n!}$. Evaluating at t then implies that the inverse of $t \cdot g(t)$ is contained in L. Since $t \cdot g(t)$ is a $\mathrm{GF}(p)$-linear combination of $t, t^2, \ldots, t^{n!} \in A$, we conclude that $t^{-1} \cdot g(t)^{-1} \in A^{-1} \cap L$, as required.

(ii) Finally assume that $|K : A| < \infty$ and that $|K| = \infty$. Now, for $i = 1, 2, \ldots, n!$, the maps $A \to K/A$ given by $x \mapsto x^i \mod A$ are polynomial forms. In particular, since A is infinite and K/A is finite, it follows from Proposition 1.3 that there exists an infinite subgroup $B \subseteq A$ on which all these maps become zero. In other words, if $x \in B$, then $x^i \in A$ for all such i. Since there are only finitely many elements of K that are roots of any polynomial over $\mathrm{GF}(p)$ of degree $\leq n!$ and since B is infinite, we can choose $t \in B$ so that $t, t^2, \ldots, t^{n!} \in A$ and such that these powers of t are linearly independent over $\mathrm{GF}(p)$. The result now follows from part (i) above. □

References

[O] J. M. Osterburg, *The zeros and the final value of a polynomial form*, Commun. Algebra **33** (2005), 2253–2262.

[P1] D. S. Passman, *Invariant ideals and polynomial forms*, Trans. AMS **354** (2002), 3379–3408.

[P2] D. S. Passman, *Invariant ideals of abelian group algebras under the action of simple linear groups*, Resenhas IME-USP **5** (2002), 377–390.

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