ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 3, 2009

GROUP ALGEBRAS OF FINITE ABELIAN GROUPS AND THEIR APPLICATIONS TO COMBINATORIAL PROBLEMS

WEIDONG GAO, ALFRED GEROLDINGER AND FRANZ HALTER-KOCH

1. Introduction and main result. Let G be an additive finite Abelian group. In the last decades group algebras $R[G]$–over suitable commutative rings R–have turned out to be powerful tools for a growing variety of questions from combinatorics and number theory. Many of them can be reduced to the problem whether for some given sequence $g_1 \cdot \ldots \cdot g_l$ over G we have

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \in R[G] \text{ for all } a_1, \ldots, a_l \in R \setminus \{0\}.$$

The present paper is devoted to this crucial problem. Before presenting our new results we recall the classical application of group algebras to the investigation of zero-sumfree sequences which is due to van Emde Boas, Kruyswijk and Olson, see [**7, 8, 19**]. Let $\mathrm{d}(G)$ denote the maximal length of a zero-sumfree sequence over G. Then $\mathrm{d}(G) + 1$ is the Davenport constant of G. For an overview of classical results concerning the Davenport constant, we refer to [**16**, Chapter 5]. Note however, that the problem of determining $\mathrm{d}(G)$ for all finite abelian groups is still wide open, see [**3, 13**].

For a commutative ring R, let $\mathrm{d}(G, R)$ denote the supremum of all $l \in \mathbf{N} \cup \{\infty\}$ having the following property:

There is some sequence $S = g_1 \cdot \ldots \cdot g_l$ of length l over G such that

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \in R[G] \text{ for all } a_1, \ldots, a_l \in R \setminus \{0\}.$$

If S is zero-sumfree, R is an integral domain, $a_1, \ldots, a_l \in R \setminus \{0\}$ and

$$f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) = \sum_{g \in G} c_g X^g,$$

2000 AMS *Mathematics subject classification.* Primary 20K01, 11B50, 05B15.
Keywords and phrases. Group algebras, finite Abelian groups, zero-sum sequence, additive Latin squares.
This work has been supported in part by NSFC with grant number 10671101 and by the Austrian Science Fund FWF (Project-No. P18779-N13).
Received by the editors on October 15, 2005, and in revised form on September 11, 2006.

DOI:10.1216/RMJ-2009-39-3-805

then $c_0 \neq 0$; hence, $f \neq 0$, and it follows that

$$\mathrm{d}(G) \leq \mathrm{d}(G, R).$$

Up to now no finite Abelian group G is known such that $\mathrm{d}(G) < \mathrm{d}(G, K)$ for all splitting fields K of G.

The following Theorem A is due to van Emde Boas, Kruyswijk and Olson (proofs in the present terminology may be found in [**16**, Theorems 5.5.5 and 5.5.9]).

Theorem A. *Let G be a finite Abelian group with $\exp(G) = n \geq 2$.*

1. *Let K be a splitting field of G with $\mathrm{char}\,(K) \nmid \exp(G)$. Then*

$$\mathrm{d}(G, K) \leq (n-1) + n \log \frac{|G|}{n},$$

and if G is cyclic, then $\mathrm{d}(G) = \mathrm{d}(G, K) = n - 1$.

2. *If G is a p-group, then $\mathrm{d}(G) = \mathrm{d}(G, \mathbf{Z}/p\mathbf{Z})$.*

For many combinatorial problems, it is sufficient to consider group algebras over fields (and this was the main approach in the past). Recall that, for any two finite Abelian groups G and G' with $|G| = |G'|$ and every splitting field K of G and G', we have $K[G] \cong K^{|G|} \cong K[G']$, but we clearly may have $\mathrm{d}(G) \neq \mathrm{d}(G')$. However, by Higman's theorem, $\mathbf{Z}[G] \cong \mathbf{Z}[G']$ implies that $G \cong G'$, see [**18**, Corollary 3.5.6 and Theorem 9.1.4]. Therefore, any combinatorial problem in G can, at least in principle, be tackled via the group algebra $\mathbf{Z}[G]$. Only recently this approach allowed refinement of some classical results on the number of zero-sum subsequences of some given sequence, see [**11**]. For more applications of group algebras to combinatorial problems, we refer to the bibliography (in particular, [**10, 12**], [**16**, Chapter 5] and also to Section 5.

In this paper, we investigate products of the form

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \in R[G]$$

over an arbitrary integral domain R. The main results are as follows (notations and definitions will be explained in detail in Sections 2 and 3).

Theorem 1.1. *Let G be a finite Abelian group, R an integral domain, $l \in \mathbf{N}$, $k \in [1,l]$, and let $g_1, \ldots, g_l \in G$ be such that $g_1, \ldots, g_k$ are independent. For $i \in [1,l]$, let $n_i = \operatorname{ord}(g_i) \geq 2$, and suppose that*

$$(*) \qquad \sum_{i=1}^{l} \frac{1}{n_i} - \sum_{i=2}^{k} (-1)^i \sum_{1 \leq \nu_1 < \ldots < \nu_i \leq k} \frac{1}{n_{\nu_1} \cdot \ldots \cdot n_{\nu_i}} < 1.$$

Then

$$f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \text{ for all } a_1, \ldots, a_l \in R.$$

If $S = g_1 \cdot \ldots \cdot g_l$ and $\mathrm{k}(S)$ denotes the cross number of S, then $(*)$ holds if either $\mathrm{k}(S) < 1$ or $\mathrm{k}(S) \leq 1$ and $k \geq 2$.

In particular, if p is the smallest prime divisor of $\exp(G)$ and $|S| < p$, then $f \neq 0$.

Corollary 1.2. *Let G be a cyclic group of order $n \geq 2$, $g_1, \ldots, g_{n-1} \in G$ and K a splitting field of G. Then the following statements are equivalent*:

(a) $(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_{n-1}} - a_{n-1}) \neq 0$ *for all* $a_1, \ldots, a_{n-1} \in K^\times$.

(b) $\operatorname{ord}(g_1) = \ldots = \operatorname{ord}(g_{n-1}) = n$.

Corollary 1.2 shows that Theorem 1.1 is sharp for cyclic groups, provided that we deal with the group algebra over a splitting field. In Example 4.2 we present a sequence $g_1 \cdot \ldots \cdot g_{p+1}$ over an elementary Abelian p-group containing two independent elements such that

$$(X^{g_1} - 1) \cdot \ldots \cdot (X^{g_{p+1}} - 1) = 0 \in R[G]$$

for any commutative ring R. Thus Theorem 1.1 is also sharp in the noncyclic case.

Consider the last statement of Theorem 1.1. In the case of p-groups, a first (but entirely different) proof was given in [**14**, Lemma 4 (ii)]. In the special case $G = \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$ and $R = \mathbf{Z}/p\mathbf{Z}$, Theorem 1.1 was first shown by Peng, see [**20, 21**], in his investigations of additive bases. Moreover, for sequences $S = g_1 \cdot \ldots \cdot g_l$ of length $l \in [p, 2p-2]$,

he gave conditions on the structure of the sequence S implying that $(X^{g_1}-1)\cdot\ldots\cdot(X^{g_l}-1)$ is either zero or nonzero.

In Section 2 we fix our notations (in particular those concerning sequences) and in Section 3 we deal with group algebras. There we establish the results which are needed for the proof of Theorem 1.1 but which are also of independent interest. The proofs of Theorem 1,1 and of Corollary 1.2 are given in Section 4. Finally, in Section 5 we apply Theorem 1.1 to a problem dealing with transversals of additive Latin squares which was recently studied by Alon et al., see [**1, 5, 14, 22, 23**].

2. Notations. Let $\mathbf{N}$ denote the set of positive integers and $\mathbf{N}_0 = \mathbf{N}\cup\{0\}$. For $a,b\in\mathbf{Z}$ we use the notation $[a,b]=\{x\in\mathbf{Z}\mid a\le x\le b\}$ (in particular, $[a,b]=\varnothing$ if $a>b$). For a finite set X, we denote by $|X|\in\mathbf{N}$ its cardinality.

Let G be a finite Abelian group (throughout, Abelian groups will be written additively). For $g\in G$, we denote by $\operatorname{ord}(g)\in\mathbf{N}$ the order of g.

If $r\in\mathbf{N}$ and $e_1,\ldots,e_r\in G\setminus\{0\}$, then the r-tuple $(e_1,\ldots,e_r)$ is called *independent* if, for all $m_1,\ldots,m_r\in\mathbf{Z}$,

$$m_1e_1+\ldots+m_re_r=0 \text{ implies that } m_1e_1=\ldots=m_re_r=0.$$

In that case, we also say that the elements $e_1,\ldots,e_r$ are independent. Concerning sequences, we adopt the terminology used in [**16**, Chapter 5]. We denote by $\mathcal{F}(G)$ the free (Abelian, multiplicative) monoid with basis G. Its elements are called *sequences over* G (indeed, the elements of $\mathcal{F}(G)$ are finite sequences of elements of G disregarding the order). In particular, $1\in\mathcal{F}(G)$ is the empty sequence.

For a sequence

$$S=g_1\cdot\ldots\cdot g_l\in\mathcal{F}(G)\ (\text{with } l\in N_0 \text{ and } g_1,\ldots,g_l\in G)$$

we call l its *length*, $\operatorname{supp}(S)=\{g_1,\ldots,g_l\}$ its *support*, $g_1+\ldots+g_l\in G$ its *sum* and

$$\mathrm{k}(S)=\sum_{i=1}^{l}\frac{1}{\operatorname{ord}(g_i)}$$

its *cross number*. A sequence $T \in \mathcal{F}(G)$ is called a *subsequence* of S, if $S = TT'$ for some sequence $T' \in \mathcal{F}(G)$. The sequence S is called *squarefree* if $g_1, \ldots, g_l$ are (pairwise) distinct, and it is called *zero-sumfree* if there is no nonempty subsequence with sum zero.

We refer to [**16**, Chapter 5] for various results concerning cross numbers and to [**2**] for some recent progress. Moreover, it was proved in [**15**] that every sequence $S \in \mathcal{F}(G)$ of length $l \geq |G|$ has a zero-sumfree subsequence T with cross number $\mathrm{k}(T) < 1$. For a graph theoretical approach, we refer to [**6**].

3. Group algebras and characters. Let R be a commutative ring (throughout, we assume that R has a unit element $1 \neq 0$) and G a finite Abelian group. The *group algebra* $R[G]$ of G over R is a free R-module with basis $\{X^g \mid g \in G\}$ (built with a symbol X), where multiplication is defined by

$$\Big(\sum_{g\in G} a_g X^g\Big)\Big(\sum_{g\in G} b_g X^g\Big) = \sum_{g\in G}\Big(\sum_{h\in G} a_h b_{g-h}\Big)X^g.$$

We view R as a subset of $R[G]$ by means of $a = aX^0$ for all $a \in R$. An element of R is a zero-divisor [a unit] of $R[G]$ if and only if it is a zero-divisor [a unit] of R.

The *augmentation map*

$$\varepsilon\colon R[G] \longrightarrow R, \text{ defined by } \varepsilon\Big(\sum_{g\in G} a_g X^g\Big) = \sum_{g\in G} a_g$$

is an epimorphism of R-algebras. For every $f \in R[G]$ the multiplication

$$\mu_f\colon R[G] \longrightarrow R[G], \text{ defined by } g \longmapsto fg \text{ for every } g \in R[G]$$

is an R-module homomorphism. Clearly, μ_f is surjective if and only if $f \in R[G]^\times$, and μ_f is injective if and only if f is not a zero-divisor of $R[G]$. Consequently, if R is a field, then every element of $R[G]$ is either a unit or a zero-divisor.

If R is an integral domain with quotient field K, then every finitely generated torsion free R-module M is contained in a vector space V

over K such that $KM = V$. In particular, M contains a K-basis of V, and we call $\mathrm{rk}\,(M) = \dim_K(V)$ the *rank* of M.

Let K be a field, $\exp(G) = n \in \mathbf{N}$ and $\mu_n(K) = \{x \in K \mid x^n = 1\}$ the group of nth roots of unity in K. An nth root of unity x is called *primitive* if $x^m \neq 1$ for all $m \in [1, n-1]$. We denote by $\mathrm{Hom}\,(G, K^\times) = \mathrm{Hom}\,(G, \mu_n(K))$ the *character group of G with values in K*. Every character $\chi \in \mathrm{Hom}\,(G, K^\times)$ has a unique extension to a K-algebra homomorphism $\chi\colon K[G] \to K$ (again denoted by χ) acting by means of

$$\chi\Big(\sum_{g\in G} a_g X^g\Big) = \sum_{g\in G} a_g \chi(g).$$

Following [**4**, Section 17], we call K a *splitting field* of G if $\mu_n(K) = \mu_n(\overline{K})$ for some algebraic closure $\overline{K}$ of K. In particular, if $\mathrm{char}\,(K) \nmid n$, then K is a splitting field of G if and only if $|\mu_n(K)| = n$, and if $\mathrm{char}\,(K) = p$ and $n = p^e m$, where e, $m \in \mathbf{N}$ and $p \nmid m$, then K is a splitting field of G if and only if $|\mu_n(K)| = m$.

If K is a splitting field of G with $\mathrm{char}\,(K) \nmid n$, then $G \cong \mathrm{Hom}\,(G, K^\times)$, the orthogonality relations hold, and for every $f \in K[G]$ we have $f = 0$ if and only if $\chi(f) = 0$ for every $\chi \in \mathrm{Hom}\,(G, K^\times)$, see [**16**, Proposition 5.5.2]. Moreover, if $\chi(f) \neq 0$ for all $\chi \in \mathrm{Hom}\,(G, K^\times)$, then $f \in K[G]^\times$ (explicitly, a simple calculation using the orthogonality relations shows that

$$f^{-1} = \frac{1}{|G|} \sum_{g\in G} \Bigg(\sum_{\chi\in \mathrm{Hom}\,(G,K^\times)} \frac{\chi(-g)}{\chi(f)} \Bigg) X^g.$$

We proceed with some simple but less common facts concerning group algebras.

Proposition 3.1. *Let G be a finite Abelian group, $g \in G$, $\mathrm{ord}\,(g) = n \in \mathbf{N}$ and R an integral domain.*

1. *If $a \in R$, then $X^g - a$ is a zero-divisor of $R[G]$ if and only if $a^n = 1$.*

2. *If $\mathrm{char}\,(R) \nmid n$, $l \in \mathbf{N}$ and $n_1, \ldots, n_l \in [1, n-1]$, then*

$$(X^{n_1 g} - 1) \cdot \ldots \cdot (X^{n_l g} - 1) \neq 0 \in R[G].$$

Proof. We may assume that $n \geq 2$. Let $R[T]$ be a polynomial ring, and let $\varphi: R[T] \to R[G]$ be the unique homomorphism of R-algebras satisfying $\varphi(T) = X^g$. Then $\mathrm{Ker}\,(\varphi) = (T^n - 1)R[T]$.

1. If $a \in R$, then

$$1 - a^n = (X^g)^n - a^n = (X^g - a)f,$$

where

$$f = \sum_{j=0}^{n-1} (X^g)^j a^{n-1-j}.$$

Since $f = \varphi(\tilde{f})$ for some polynomial $\tilde{f} \in R[T]$ of degree less than n, we obtain $f \neq 0$.

If $a^n = 1$, then $(X^g - a)f = 0$, and thus $X^g - a$ is a zero-divisor of $R[G]$. If $a^n \neq 1$, then $a^n - 1 \neq 0$ and thus $a^n - 1$ is not a zero-divisor of $R[G]$. Hence also $X^g - a$ is not a zero-divisor of $R[G]$.

2. We must prove that

$$(T^{n_1} - 1) \cdot \ldots \cdot (T^{n_l} - 1) \notin (T^n - 1)R[T].$$

Since $\mathrm{char}\,(R) \nmid n$, there exists a primitive nth root of unity ω in some field containing R. Then $\omega^n - 1 = 0$ and $\omega^{n_i} - 1 \neq 0$ for all $i \in [1, l]$, whence the assertion follows. □

Proposition 3.2. *Let G be a finite Abelian p-group.*

1. *Let R be an integral domain of characteristic p and $f \in R[G]$. Then we have $f \in R[G]^\times$ if and only if $\varepsilon(f) \in R^\times$.*

2. *If $f \in \mathbf{Z}[G]$ and $\varepsilon(f) \notin p\mathbf{Z}$, then f is not a zero-divisor of $\mathbf{Z}[G]$.*

Proof. Let $n = \exp(G)$.

1. Since $(X^g)^n = 1$ for all $g \in G$, we obtain $f^n = \varepsilon(f)^n$ for all $f \in R[G]$, and consequently we have $f \in R[G]^\times$ if and only if $\varepsilon(f) \in R[G]^\times \cap R = R^\times$.

2. Let $\varphi: \mathbf{Z}[G] \to \mathbf{Z}/p\mathbf{Z}[G]$ be the canonical epimorphism. Then $\varepsilon(\varphi(f)) = \varphi(\varepsilon(f)) \neq 0$ and thus $\varphi(f) \in \mathbf{Z}/p\mathbf{Z}[G]^\times$ by 1. Assume now that f is a zero-divisor in $\mathbf{Z}[G]$. Then there exists some $g \in \mathbf{Z}[G]$ such

that $g \neq 0$ and $fg = 0$, and we may assume that $g \notin p\mathbf{Z}[G]$. Then $\varphi(g) \neq 0$ and $\varphi(f)\varphi(g) = \varphi(fg) = 0$, a contradiction. □

4. Proofs of Theorem 1.1 and of Corollary 1.2. Proposition 4.1 is crucial for the proofs of Theorem 1.1 and Corollary 1.2.

Proposition 4.1. *Let G be a finite Abelian group, R a commutative ring, $k \in \mathbf{N}$, $g_1, \dots, g_k \in G$, $a_1, \dots, a_k \in R$ and*

$$V = \big\{ b \in R[G] \;\big|\; (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k) b = 0 \big\}.$$

1. *An element*

$$b = \sum_{\sigma \in G} b(\sigma) X^\sigma \in R[G]$$

lies in V if and only if, for all $\sigma \in G$ and $m_1, \dots, m_k \in \mathbf{N}$, we have

$$\text{(A)} \quad (-1)^{k-1} \Big(\prod_{i=1}^k a_i^{m_i} \Big) b\Big(\sigma + \sum_{i=1}^k m_i g_i \Big) = \sum_{j=0}^{k-1} (-1)^j \sum_{\substack{I \subset [1,k] \\ |I| = j}} \Big(\prod_{i \in I} a_i^{m_i} \Big) b\Big(\sigma + \sum_{i \in I} m_i g_i \Big).$$

2. *Let $g_1, \dots, g_k \in G$ be independent with $\operatorname{ord}(g_i) = n_i \geq 2$ and $a_i^{n_i} = 1$ for all $i \in [1,k]$. Let $\Omega \subset G$ be a set of representatives for $G/\langle g_1, \dots, g_k \rangle$ and M the set of all $(k+1)$-tuples $(\tau, m_1, \dots, m_k)$, where $\tau \in \Omega$, $m_1, \dots, m_k \in [0, n_i - 1]$ for all $i \in [1,k]$ and $m_i = 0$ for at least one $i \in [1,k]$. Then we have:*

For every family $(a(\tau, m_1, \dots, m_k))_{(\tau, m_1, \dots, m_k) \in M} \in R^M$, there exists a unique $b \in V$ such that

$$b\Big(\tau + \sum_{i=1}^k m_i g_i \Big) = a(\tau, m_1, \dots, m_k) \text{ for all } (\tau, m_1, \dots, m_k) \in M.$$

In particular, V is a free R-module and

$$\operatorname{rk}(V) = |M| = |G| \Big(1 - \prod_{i=1}^k \Big(1 - \frac{1}{n_i} \Big) \Big).$$

Proof. 1. We set

$$\prod_{i=1}^{k}(X^{g_i}-a_i)\sum_{\sigma\in G}b(\sigma)X^{\sigma}=\sum_{\sigma\in G}b_k(\sigma)X^{\sigma},$$

and we prove by induction on k that for all $\sigma\in G$ we have

$$\text{(P)}\qquad b_k\Big(\sigma+\sum_{i=1}^{k}g_i\Big)=\sum_{j=0}^{k}(-1)^j\sum_{\substack{I\subset[1,k]\\|I|=j}}\Big(\prod_{i\in I}a_i\Big)\,b\Big(\sigma+\sum_{i\in I}g_i\Big).$$

For $k=0$, there is nothing to do.

$k\geq 1$, $k-1\to k$. We have

$$(X^{g_k}-a_k)\sum_{\sigma\in G}b_{k-1}(\sigma)X^{\sigma}=\sum_{\sigma\in G}\Big(b_{k-1}(\sigma-g_k)-a_kb_{k-1}(\sigma)\Big)X^{\sigma};$$

hence, $b_k(\sigma)=b_{k-1}(\sigma-g_k)-a_kb_{k-1}(\sigma)$ and therefore, for all $\sigma\in G$,

$$b_k\Big(\sigma+\sum_{i=1}^{k}g_i\Big)=b_{k-1}\Big(\sigma+\sum_{i=1}^{k-1}g_i\Big)-a_k\,b_{k-1}\Big(\sigma+g_k+\sum_{i=1}^{k-1}g_i\Big).$$

Together with the induction hypothesis, this implies (P).

By definition, we have $b\in V$ if and only if $b_k(\sigma)=0$ for all $\sigma\in G$, or, equivalently, $b_k(\sigma+g_1+\ldots+g_k)=0$ for all $\sigma\in G$. By (P), this is true if and only if (A) holds for $m_1=\cdots=m_k=1$. Thus it remains to prove that (A) holds for all $(m_1,\ldots,m_k)\in\mathbf{N}^k$ provided that it holds for $(1,\ldots,1)\in\mathbf{N}^k$.

If $(m_1,\ldots,m_k)\in\mathbf{N}^k$ and (A) holds for $(1,\ldots,1)\in\mathbf{N}^k$, then the associated element b lies in V and $(X^{g_1}-a_1)\cdot\ldots\cdot(X^{g_k}-a_k)b=0$. This implies that

$$(X^{m_1g_1}-a_1^{m_1})\cdot\ldots\cdot(X^{m_kg_k}-a_k^{m_k})b=0,$$

and thus (A) holds for $(m_1,\ldots,m_k)\in\mathbf{N}^k$.

2. Let $(a(\tau,m_1,\ldots,m_k))_{(\tau,m_1,\ldots,m_k)\in M}\in R^M$ be given. By 1 there exists a unique map $b\colon\overline{M}=\Omega\times[0,n_1-1]\times\ldots\times[0,n_k-1]\to R$ such that

$b(\tau, m_1, \dots, m_k) = a(\tau, m_1, \dots, m_k)$ for all $(\tau, m_1, \dots, m_k) \in M$ and (A) holds for all $(\sigma, m_1, \dots, m_k) \in \Omega \times [1, n_1 - 1] \times \dots \times [1, n_k - 1]$. Since $g_1, \dots, g_k$ are independent, every $\sigma \in G$ has a unique representation

$$\sigma = \tau + \sum_{i=1}^{k} m_i g_i \text{ with } (\tau, m_1, \dots, m_k) \in \overline{M},$$

and we define $b^*(\sigma) = b(\tau, m_1, \dots, m_k)$ and

$$b^* = \sum_{\sigma \in G} b^*(\sigma) X^\sigma.$$

Since $a_i^{n_i} = 1$ for all $i \in [1, k]$, it follows that (A) holds for all $\sigma \in G$ and $m_1, \dots, m_k \in \mathbf{N}$, and consequently 1 implies that $b^* \in V$. Hence the assignment

$$\Big(a(\tau, m_1, \dots, m_k)\Big)_{(\tau, m_1, \dots, m_k) \in M} \longmapsto b^*$$

defines an isomorphism $R^M \xrightarrow{\sim} V$, and thus we have

$$|M| = |\Omega| \left(\prod_{i=1}^{k} n_i - \prod_{i=1}^{k} (n_i - 1) \right) \text{ and } |\Omega| = \frac{|G|}{n_1 \cdot \ldots \cdot n_k}. \qquad \square$$

Proof of Theorem 1.1. We may suppose that R is a field. If $a_i^{n_i} \neq 1$ for some $i \in [1, l]$, then Proposition 3.1 implies that $X^{g_i} - a_i \in R[G]^\times$, and thus we may assume that $a_i^{n_i} = 1$ for all $i \in [1, l]$. If $V = \{b \in R[G] \mid (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k) b = 0\}$, then Proposition 4.1 implies that

$$\dim_R(V) = |G| \left(1 - \prod_{i=1}^{k} \left(1 - \frac{1}{n_i} \right) \right),$$

and therefore

$$\dim_R (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k) R[G] = |G| - \dim_R V = |G| \prod_{i=1}^{k} \left(1 - \frac{1}{n_i} \right).$$

For $i \in [k+1, l]$ we set $V_i = \{b \in R[G] \mid (X^{g_i} - a_i)b = 0\}$, and again Proposition 4.1 implies that

$$\dim_R(V_i) = |G| \frac{1}{n_i}$$

and therefore

$$\dim_R(X^{g_i} - a_i)R[G] = |G| - \dim_R V_i = |G|\left(1 - \frac{1}{n_i}\right).$$

If U is any finite-dimensional vector space over R, $l \in \mathbf{N}$ and $\lambda_1, \ldots, \lambda_l : U \to U$ are R-linear, then it is easily proved by induction that

$$\dim_R(\lambda_1 \circ \ldots \circ \lambda_l)(U) \geq \sum_{i=1}^{l} \dim_R \lambda_i(U) - (l-1)\dim(U).$$

Hence we obtain

$$\begin{aligned}
&\dim_R(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l)\, R[G] \\
&\quad \geq \dim_R(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k)\, R[G] \\
&\qquad + \sum_{i=k+1}^{l} \dim_R(X^{g_i} - a_i)\, R[G] - (l-k)|G| \\
&\quad \geq |G| \prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right) + \sum_{i=k+1}^{l} |G|\left(1 - \frac{1}{n_i}\right) - (l-k)|G| \\
&\quad = |G|\left[\prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right) - \sum_{i=k+1}^{l} \frac{1}{n_i}\right] \\
&\quad = |G|\left[1 - \sum_{i=1}^{l} \frac{1}{n_i} + \sum_{i=2}^{k} (-1)^i \sum_{1 \leq \nu_1 < \ldots < \nu_i \leq k} \frac{1}{n_{\nu_1} \cdot \ldots \cdot n_{\nu_i}}\right] > 0,
\end{aligned}$$

and therefore $(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0$. This proves the main assertion.

As to the assertions concerning the cross number, observe that

$$\mathrm{k}(S) = \sum_{i=1}^{l} \frac{1}{n_i}$$

and

$$\sum_{i=2}^{k}(-1)^i \sum_{1\le\nu_1<\ldots<\nu_i\le k} \frac{1}{n_{\nu_1}\cdot\ldots\cdot n_{\nu_i}} = \prod_{i=1}^{k}\left(1-\frac{1}{n_i}\right) - 1 + \sum_{i=1}^{k}\frac{1}{n_i} \ge 0,$$

with equality if and only if $k = 1$.

If p is the smallest prime divisor of $\exp(G)$ and $|S| < p$, then

$$\mathrm{k}(S) = \sum_{i=1}^{l}\frac{1}{\mathrm{ord}\,(g_i)} \le \frac{l}{p} < 1,$$

which proves the last assertion. □

Proof of Corollary 1.2. (b) $\Rightarrow$ (a). By Theorem 1.1.

(a) $\Rightarrow$ (b). Assume to the contrary that $\mathrm{ord}\,(g_i) < n$ for some $i \in [1, n-1]$, say $\mathrm{ord}\,(g_1) < n$. We shall prove that there exist $a_1, \ldots, a_{n-1} \in \mu_n(K)$ satisfying

$$(X^{g_1} - a_1)\cdot\ldots\cdot(X^{g_{n-1}} - a_{n-1}) = 0.$$

Case 1. $\mathrm{char}\,(K) \nmid n$. Let $\Omega = \{\chi \in \mathrm{Hom}\,(G, K^\times) \mid \chi(g_1) \ne 1\}$. Since $\mathrm{ord}\,(g_1) < n$, it follows that $\chi(g_1) = 1$ for at least one nontrivial character $\chi \in \mathrm{Hom}\,(G, K^\times)$, and thus we obtain $|\Omega| \le n-2$, say $\Omega = \{\chi_2, \ldots, \chi_s\}$, where $s \in [1, n-1]$ and $|\Omega| = s-1$. If

$$f = (X^{g_1} - 1)\prod_{i=2}^{s}\left(X^{g_i} - \chi_i(g_i)\right)\prod_{i=s+1}^{n-1}(X^{g_i} - 1) \in K[G],$$

then $\chi(f) = 0$ for all $\chi \in \mathrm{Hom}\,(G, K^\times)$ and thus $f = 0$.

Case 2. $\mathrm{char}\,(K) \mid n$. Let $\mathrm{char}\,(K) = p$ and $n = p^e m$, where e, $m \in \mathbf{N}$ and $p \nmid m$. Then K contains the field F of mth roots of unity over its prime field, and we may assume that $K = F$. Let $\zeta \in \mathbf{C}$ be a primitive nth root of unity, $L = \mathbf{Q}(\zeta)$, R the ring of integers in

L and $\mathfrak{p}$ a maximal ideal of R with $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Then $R/\mathfrak{p} \cong K$, see [**17**, Chapter IV.1], and we denote by $\varphi\colon R[G] \to K[G]$ the canonical epimorphism. By Case 1 there exist $a_1, \dots, a_{n-1} \in \mu_n(L)$ such that $f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_{n-1}} - a_{n-1}) = 0$, and as $\mu_n(L) \subset R \setminus \mathfrak{p}$, it follows that $\varphi(a_1), \dots, \varphi(a_{n-1}) \in K^\times$ and

$$0 = \varphi(f) = \left(X^{g_1} - \varphi(a_1)\right) \cdot \ldots \cdot \left(X^{g_{n-1}} - \varphi(a_{n-1})\right) \in K[G]. \qquad \square$$

Next we provide the announced example of a sequence $g_1 \cdot \ldots \cdot g_{p+1}$ in an elementary Abelian p-group containing two independent elements such $(X^{g_1} - 1) \cdot \ldots \cdot (X^{g_{p+1}} - 1) = 0 \in \mathbf{Z}[G]$.

Example 4.2. Let G be an elementary Abelian p-group (for an arbitrary prime p), $g, h \in G$ two independent elements, R a commutative ring,

$$S = gh \prod_{i=1}^{p-1} (g + ih) \in \mathcal{F}(G)$$

and

$$f = (1 - X^g)(1 - X^h) \prod_{i=1}^{p-1} (1 - X^{g+ih}) \in R[G].$$

We shall prove that $f = 0$. Since there is a natural homomorphism $\varphi\colon \mathbf{Z}[G] \to R[G]$, we may suppose that $R = \mathbf{Z}$, and clearly, it suffices to show that $f = 0 \in K[G]$ for some algebraic number field K. Let K be the field of pth roots of unity over $\mathbf{Q}$. Then K is a splitting field of G, and it suffices to prove that $\chi(f) = 0$ for all $\chi \in \mathrm{Hom}\,(G, K^\times)$. Thus, let $\chi \in \mathrm{Hom}\,(G, K^\times)$. If $\chi(g) = 1$ or $\chi(h) = 1$, then obviously $\chi(f) = 0$. Thus we may assume that $\chi(g) = \zeta$ and $\chi(h) = \zeta^k$, where $\zeta \in K$ is a primitive pth root of unity and $k \in [1, p-1]$. Then there is some $i \in [1, k-1]$ such that $ki + 1 \equiv 0 \bmod p$ and

$$\chi(f) = (1 - \zeta)(1 - \zeta^k) \prod_{i=1}^{p-1} (1 - \zeta^{ik+1}) = 0. \qquad \square$$

5. Transversals of additive Latin squares. In this section we apply our main result on group algebras to the problem of finding large Latin transversals in Cayley matrices of Abelian groups. We do not recall these combinatorial notions but describe the problem in completely elementary terms. In fact, we start with a slightly more general approach. For $l \in \mathbf{N}$, let $\mathfrak{S}_l$ denote the group of permutations of $[1, l]$.

Let G be an additive Abelian group and $l \in \mathbf{N}$. We say that l has property (P) (for G) if

for every squarefree sequence $g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ and every sequence $h_1 \cdot \ldots \cdot h_l \in \mathcal{F}(G)$, there is some permutation $\pi \in \mathfrak{S}_l$ such that the sequence $(g_1 + h_{\pi(1)}) \cdot \ldots \cdot (g_l + h_{\pi(l)})$ is squarefree.

If G is torsionfree, then every $l \in \mathbf{N}$ has property (P). Indeed, there is a total order $<$ on G. If $g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ is a squarefree sequence and $h_1 \cdot \ldots \cdot h_l \in \mathcal{F}(G)$ is any sequence then (after renumbering if necessary) we may assume that $g_1 < \ldots < g_l$ and $h_1 \le \ldots \le h_l$, whence $g_1 + h_1 < \ldots < g_l + h_l$ and thus $(g_1 + h_1) \cdot \ldots \cdot (g_l + h_l)$ is squarefree.

Now let $g \in G$ be an element of order $l \in \mathbf{N}$. If $g_i = (i-1)g$ for $i \in [1, l]$, $h_i = 0$ for $i \in [1, l-1]$ and $h_l = g$, then the sequence $g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ is squarefree, but there is no permutation such that the sequence $(g_1 + h_1) \cdot \ldots \cdot (g_l + h_l)$ is squarefree. In particular, if G has some element of order 2, then the 1 is the only integer with Property (P).

Conjecture (see [**5**, page 23] and [**22**, Conjecture 3]). *If G is a finite Abelian group of odd order and p is the smallest prime divisor of* $\exp(G)$*, then every $l \in [1, p-1]$ has Property* (P).

This conjecture was first proved for prime cyclic groups by Alon [**1**], and then for cyclic groups of prime power order and for elementary p-groups by Dasgupta et al. [**5**, Theorem 2]. Theorem 1.1 and a crucial combinatorial lemma by Dasgupta (Proposition 5.1) offer a new approach to this problem which we present in Theorem 5.2 and in Corollary 5.3 (statements 2 and 3 of Corollary 5.3 were first obtained in [**14**]).

Let A be a commutative ring and $l \in \mathbf{N}$. For $x_1, \ldots, x_l \in A$, let

$$V(x_1, \ldots, x_l) = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_l \\ \vdots & \vdots & \vdots \\ x_1^{l-1} & \cdots & x_l^{l-1} \end{pmatrix}$$

denote the Vandermonde matrix, and for some (l,l)-matrix $M = (x_{i,j})_{i,j\in[1,l]}$ over A, let

$$\operatorname{Per} M = \sum_{\pi\in\mathfrak{S}_l} x_{1,\pi(1)} \cdot \ldots \cdot x_{l,\pi(l)} \in A,$$

denote the permanent of M. In subsequent applications we will deal with the group algebra $A = \mathbf{Z}[G]$ for some Abelian group G.

Proposition 5.1. *Let A be a commutative ring, $l \in \mathbf{N}$ and $x_1, \ldots, x_l, y_1, \ldots, y_l \in A$. Then*

$$\sum_{\pi\in\mathfrak{S}_l} \prod_{1\le i<j\le l} (x_j y_{\pi(j)} - x_i y_{\pi(i)}) = \operatorname{Det} V(x_1, \ldots, x_l) \operatorname{Per} V(y_1, \ldots, y_l).$$

Proof. This follows from [**5**, Lemma 5]. □

Theorem 5.2. *Let G be a finite Abelian group of odd order, $l \in \mathbf{N}$, $g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ a squarefree sequence and $h_1 \cdot \ldots \cdot h_l \in \mathcal{F}(G)$ any sequence of length l. In each of the following cases there exists some permutation $\pi \in \mathfrak{S}_l$ such that the sequence $(g_1 + h_{\pi(1)}) \cdot \ldots \cdot (g_l + h_{\pi(l)})$ is squarefree*:

1. *G is a p-group, $l < p$ and $\operatorname{Det} V(X^{g_1}, \ldots, X^{g_l}) \neq 0 \in \mathbf{Z}[G]$.*
2. *G is cyclic, and $\operatorname{Per} V(X^{h_1}, \ldots, X^{h_l})$ is not a zero-divisor in $\mathbf{Z}[G]$.*
3. *For the sequence*

$$S = \prod_{1\le i<j\le l} (g_j - g_i)(h_j - h_i) \in \mathcal{F}(G),$$

we have either $\mathrm{k}(S) < 1$, or $\mathrm{k}(S) \le 1$ and $\operatorname{supp}(S)$ contains at least two independent elements.

Proof. By Proposition 5.1, we have

$$\operatorname{Det} V(X^{g_1}, \dots, X^{g_l}) \operatorname{Per} V(X^{h_1}, \dots, X^{h_l}) = \sum_{\pi \in \mathfrak{S}_l} \prod_{1 \le i < j \le l} (X^{g_j + h_{\pi(j)}} - X^{g_i + h_{\pi(i)}}),$$

and it suffices to prove that $\operatorname{Det} V(X^{g_1}, \dots, X^{g_l}) \operatorname{Per} V(X^{h_1}, \dots, X^{h_l}) \neq 0$. Indeed, then there exists some $\pi \in \mathfrak{S}_l$ such that

$$\prod_{1 \le i < j \le l} (X^{g_j + h_{\pi(j)}} - X^{g_i + h_{\pi(i)}}) \neq 0,$$

whence the sequence $(g_1 + h_{\pi(1)}) \cdot \ldots \cdot (g_l + h_{\pi(l)})$ is squarefree.

1. By the very definition of the permanent, we have $\varepsilon(\operatorname{Per} V(X^{h_1}, \dots, X^{h_l})) = l! \notin p\mathbf{Z}$. Hence, $\operatorname{Per} V(X^{h_1}, \dots, X^{h_l})$ is not a zero-divisor in $\mathbf{Z}[G]$ by Proposition 3.2, and thus

$$\operatorname{Det} V(X^{g_1}, \dots, X^{g_l}) \operatorname{Per} V(X^{h_1}, \dots, X^{h_l}) \neq 0.$$

2. It suffices to prove that $\operatorname{Det} V(X^{g_1}, \cdots, X^{g_l}) \neq 0$. By Proposition 3.1 we have

$$\prod_{1 \le i < j \le l} (X^{g_j - g_i} - 1) \neq 0,$$

and since $X^{g_i} \in \mathbf{Z}[G]^\times$ for all $i \in [1, l]$, we obtain

$$\operatorname{Det} V(X^{g_1}, \cdots, X^{g_l}) = \prod_{1 \le i < j \le l} (X^{g_j} - X^{g_i}) = \prod_{1 \le i < j \le l} X^{g_i} (X^{g_j - g_i} - 1) \neq 0.$$

3. We view the matrices $V(X^{g_1}, \dots, X^{g_l})$ and $V(X^{h_1}, \dots, X^{h_l})$ as matrices over $K[G]$, where $K = \mathbf{Z}/2\mathbf{Z} = \{\overline{0}, \overline{1}\}$ denotes the field with two elements. Then it suffices to prove that

$$f = \operatorname{Det} V(X^{g_1}, \dots, X^{g_l}) \operatorname{Per} V(X^{h_1}, \dots, X^{h_l}) \neq 0 \in K[G].$$

We obtain

$$\begin{aligned} f &= \operatorname{Det} V(X^{g_1}, \cdots, X^{g_l}) \operatorname{Det} V(X^{h_1}, \cdots, X^{h_l}) \\ &= \prod_{1 \le i < j \le l} (X^{g_j} - X^{g_i}) \prod_{1 \le i < j \le l} (X^{h_j} - X^{h_i}) \\ &= \prod_{1 \le i < j \le l} X^{g_i + h_i} (X^{g_j - g_i} - \overline{1})(X^{h_j - h_i} - \overline{1}) \neq 0, \end{aligned}$$

since $X^{g_i+h_i} \in K[G]^\times$ for all $i \in [1,l]$ and

$$\prod_{1\le i<j\le l} (X^{g_j-g_i} - \overline{1})(X^{h_j-h_i} - \overline{1}) \neq 0 \text{ by Theorem 1.1.} \qquad \square$$

Corollary 5.3. *Let G be a finite Abelian group of odd order, $l \in \mathbf{N}$, $g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ a squarefree sequence and $h_1 \cdot \ldots \cdot h_l \in \mathcal{F}(G)$ any sequence of length l. In each of the following cases there exists some permutation $\pi \in \mathfrak{S}_l$ such the sequence $(g_1 + h_{\pi(1)}) \cdot \ldots \cdot (g_l + h_{\pi(l)})$ is squarefree*:

1. *G is a p-group, $l < p$, and for the sequence*

$$S = \prod_{1\le i<j\le l} (g_j - g_i) \text{ we have } k(S) < 1.$$

2. *G is a p-group and $2l < 1 + \sqrt{8p+1}$.*

3. *The sequence $h_1 \cdot \ldots \cdot h_l$ is squarefree, and $2l < 1 + \sqrt{4p+1}$, where p denotes the smallest prime divisor of $|G|$.*

Proof. 1. We have

$$\operatorname{Det} V(X^{g_1}, \cdots, X^{g_l}) = \prod_{1\le i<j\le l} X^{g_i} \prod_{1\le i<j\le l} (X^{g_j-g_i} - 1).$$

Since the first factor is a unit in $\mathbf{Z}[G]$, and the second factor is nonzero by Theorem 1.1, the assertion follows by Theorem 1.1.

2. Since

$$\mathrm{k}(S) = \sum_{1\le i<j\le l} \left(\frac{1}{\operatorname{ord}(g_j - g_i)} \right) \le \frac{1}{p} \binom{l}{2} < 1,$$

the assertion follows from 1.

3. Since both $g_1 \cdot \ldots \cdot g_l$ and $h_1 \cdot \ldots \cdot h_l$ are squarefree, it follows that the sequence

$$S = \prod_{1\le i<j\le l} (g_j - g_i)(h_j - h_i) \in \mathcal{F}(G)$$

satisfies

$$\mathrm{k}(S) = \sum_{1 \le i < j \le l} \left(\frac{1}{\mathrm{ord}\,(g_j - g_i)} + \frac{1}{\mathrm{ord}\,(h_j - h_i)} \right) \le \frac{2}{p} \binom{l}{2} < 1,$$

whence the assertion follows from Theorem 5.2.3. □

Note added in proof. When this article went to press in spring 2009, we were informed on much recent progress (achieved by Zhi-Wei Sun et al. [**9**]) on Snevily's conjecture and a conjecture by Dasgupta-Károlyi-Serra-Szegedy [**24**].

Acknowledgments. We are indebted to Florian Kainrath who pointed out an incorrectness in a former proof of Proposition 4.1. This work was completed when the first author visited the Fields Institute of Canada and he would like to thank them for their support and hospitality.

REFERENCES

1. N. Alon, *Additive Latin transversals*, Israel J. Math. **117** (2000), 125–130.

2. P. Baginski, S.T. Chapman, K. McDonald and L. Pudwell, *On cross numbers of minimal zero sequences in certain cyclic groups*, Ars Comb. **70** (2004), 47–60.

3. S.T. Chapman, M. Freeze, W. Gao and W.W. Smith, *On Davenport's constant of finite abelian groups*, Far East J. Math. Sci. **5** (2002), 47–54.

4. C.W. Curtis and I. Reiner, *Methods of representation theory*, Volume I, John Wiley & Sons, New York, 1981.

5. S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares*, Israel J. Math. **126** (2001), 17–28.

6. S. Elledge and G.H. Hurlbert, *An application of graph pebbling to zero-sum sequences in abelian groups*, Integers **5** (2005).

7. P. van Emde Boas, *A combinatorial problem on finite abelian groups* II, Reports ZW-1969-007, Math. Centre, Amsterdam, 1969.

8. P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups* III, Reports ZW-1969-008, Math. Centre, Amsterdam, 1969.

9. T. Feng, Z.W. Sun and Q. Xiang, *Exterior algebras and two conjectures on finite abelian groups*, preprint, 2008.

10. W. Gao, *Addition theorems and group rings*, J. Comb. Theory **77** (1997), 98–109.

11. W. Gao and A. Geroldinger, *On the number of subsequences with given sum of sequences over finite abelian p-groups*, Rocky Mountain J. Math. **37** (2007), 1541–1550.

12. W. Gao and A. Geroldinger, *Zero-sum problems and coverings by proper cosets*, European J. Comb. **24** (2003), 531–549.

13. ———, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. **24** (2006), 337–369.

14. W. Gao and D.J. Wang, *Additive Latin transversals and group rings*, Israel J. Math. **140** (2004), 375–380.

15. A. Geroldinger, *On a conjecture of Kleitman and Lemke*, J. Number Theory **44** (1993), 60–65.

16. A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure Appl. Math. **278**, Chapman & Hall/CRC, 2006.

17. S. Lang, *Algebraic number theory*, 2nd ed., Springer, 1994.

18. C.P. Milies and S.K. Sehgal, *An introduction to group rings*, Kluwer Academic Publishers, New York, 2002.

19. J.E. Olson, *A combinatorial problem on finite abelian groups* I, J. Number Theory **1** (1969), 8–10.

20. C. Peng, *Addition theorems in elementary abelian groups* I, J. Number Theory **27** (1987), 46–57.

21. ———, *Addition theorems in elementary abelian groups* II, J. Number Theory **27** (1987), 58–62.

22. H.S. Snevily, *Unsolved problems: The Cayley addition table of* $\mathbf{Z}_n$, Amer. Math. Monthly **106** (1999), 584–585.

23. Zhi-Wei Sun, *On Snevily's conjecture and restricted sumsets*, J. Comb. Theory Ser. A **103** (2003), 291–304.

24. ———, *An additive theorem and restricted sumsets*, Math. Res. Letters **15** (2008), 1263–1276.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
Email address: wdgao_1963@yahoo.com.cn

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria
Email address: alfred.geroldinger@uni-graz.at

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria
Email address: franz.halterkoch@uni-graz.at