.

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

WEIDONG GAO AND ALFRED GEROLDINGER

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 $S = g_1 \cdot \ldots \cdot g_l$ over G the elements

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

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 P. van Emde Boas, D. Kruyswijk and J.E. Olson (see [8], [9],[20]).

Let $\mathsf{d}(G)$ denote the maximal length of a zero-sumfree sequence over G. Then $\mathsf{d}(G)+1$ is the Davenport constant of G. For some commutative ring R, let $\mathsf{d}(G,R)$ denote the largest integer $l \in \mathbb{N}$ having the following property: there is some sequence S over G of length $|S| = l$ such that

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

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

$$f \;=\; \sum_{g \in G} c_g X^g \;=\; \prod_{i=1}^{l} (X^{g_i} - a_i)\,,$$

then $c_0 \neq 0$ whence $f \neq 0$ and

$$\mathsf{d}(G) \le \mathsf{d}(G,R)\,.$$

The following result is due to the above authors (for proofs in the present terminology we refer to [16, Theorems 5.5.5 and 5.5.9]). Recall that the problem of determining $\mathsf{d}(G)$ is still wide open (see [5] and [13]), and up to now there is known no finite abelian group G such that $\mathsf{d}(G) < \mathsf{d}(G,K)$ for all splitting fields K of G.

Theorem A. Let G be a finite abelian group with $\exp(G) = n \ge 2$.

1. Let K be a splitting field of G. Then

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

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

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

2000 *Mathematics Subject Classification.* 20K01, 11B50, 05B15.

Key words 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 10271080.

In the past group algebras were considered mainly over fields (in connection with combinatorial problems). Whereas this is sufficient for some applications we cannot restrict to fields in general. Recall that for every finite abelian group G' with $|G'| = |G|$ and every splitting field K of G we have $K[G] \cong K^{|G|} \cong K[G']$ but clearly we may have $\mathsf{d}(G) \neq \mathsf{d}(G')$. However, by G. Higman's Theorem, $\mathbb{Z}[G] \cong \mathbb{Z}[G']$ implies that $G \cong G'$ for any group 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 $\mathbb{Z}[G]$. Only recently this approach allowed to refine some classical results on the number of zero-sum subsequences of some given sequences (see [11]). For more applications of group algebras to combinatorial problems we refer to the bibliography (in particular, [10], [16, Chapter 5], [12]) and also to Section 5.

Here are the main results of the present paper.

Theorem 1.1. *Let G be a finite abelian group, $l \in \mathbb{N}$, $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ a sequence over G, $\mathsf{k}(S) = \operatorname{ord}(g_1)^{-1} + \ldots + \operatorname{ord}(g_l)^{-1}$ its cross number and R an integral domain. If $\mathsf{k}(S) < 1$, then*

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

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 $n \geq 2$, $S = g_1 \cdot \ldots \cdot g_{n-1} \in \mathcal{F}(G)$ 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) $\operatorname{ord}(g_1) = \ldots = \operatorname{ord}(g_{n-1}) = n$.

Note that every sequence $S^* \in \mathcal{F}(G)$ of length $|S^*| \geq |G|$ has a zero-sumfree subsequence S with cross number $\mathsf{k}(S) < 1$ (see [15], [7] for a graph theoretical approach and [3] for recent progress on cross numbers). If $\operatorname{char}(R) = p$, $g \in G$ with $\operatorname{ord}(g) = p$ and $S = g^p$, then $\mathsf{k}(S) = 1$ and $(X^g - 1)^p = 0$ whence the assumption $\mathsf{k}(S) < 1$ cannot be weakened in general. Consider the additional statement of Theorem 6.3. In the case of p-groups, a first (but entirely different) proof was given in [14, Lemma 4 (ii)]. In the special case $G = C_p \oplus C_p$ and $R = \mathbb{Z}/p\mathbb{Z}$, Theorem 6.3 was first shown by C. Peng (see [21, 22]) in his investigations of additive bases. Moreover, for sequences S of length $|S| = l \in [p, 2p-2]$ 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 non-zero (in case $p = 2$ it is straightforward that there are sequences S of length $|S| = 2$ for which the conclusion of Theorem 6.3 holds resp. does not hold, and clearly this depends also on the characteristic of the ring). In Example 4.1 we provide a sequence $S \in \mathcal{F}(G)$ of length $|S| = l = p + 1$ such that, for any commutative ring R, we have $(X^{g_1} - 1) \cdot \ldots \cdot (X^{g_l} - 1) = 0 \in R[G]$.

In Section 3 we deal with group algebras and establish results which are needed for the proof of Theorem 6.3 but which are also of independent interest. The proofs of Theorem 6.3 and of Corollary 1.2 are given in Section 4. In the last section we apply Theorem 6.3 to a problem dealing with transversals of additive Latin squares which was recently studied by N. Alon et. al. (see [1], [23], [6], [24] and [14]).

2. Notations

In this section we fix some basic notations and our conventions on sequences. Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of all prime numbers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For integers $a, b \in \mathbb{Z}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$, and for $c \in \mathbb{N}$ let $\mathbb{N}_{\ge c} = \mathbb{N} \setminus [1, c-1]$. Throughout, all abelian groups will be written additively and for $n \in \mathbb{N}$ let C_n denote a cyclic group with n elements.

Let G be a finite abelian group with $\exp(G) = n$. If $r \in \mathbb{N}$ 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 $m_1, \ldots, m_r \in \mathbb{Z}$,

$$m_1 e_1 + \ldots + m_r e_r = 0 \quad \text{implies that} \quad m_1 e_1 = \ldots = m_r e_r = 0\,.$$

In that case, we also say that the elements $e_1, \ldots, e_r$ are independent.

We denote by $\mathcal{F}(G)$ the free (abelian, multiplicative) monoid with basis G. An element $S \in \mathcal{F}(G)$ is called a *sequence over* G and will be written in the form

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)} = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)\,,$$

where $\mathsf{v}_g(S)$ is called the *multiplicity of* g *in* S. As usual,

$$\sigma(S) = \sum_{g \in G} \mathsf{v}_g(S) g = \sum_{i=1}^{l} g_i \ \in \ G$$

denotes the *sum of* S,

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

is the *cross number of* S and

$$|S| = \sum_{g \in G} \mathsf{v}_g(S) = l \in \mathbb{N}_0$$

denotes the *length of* S.

3. Group algebras and characters

Let R be a commutative ring (by a ring, we always mean a ring with unit element). The *group algebra* $R[G]$ of the group G over the ring 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 $a \in R$. The *augmentation map*

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

is an epimorphism of R-algebras. Its kernel $\mathrm{Ker}(\varepsilon) = I_G$ is called the *augmentation ideal*, and $\{1 - X^g \mid 0 \neq g \in G\}$ is an R-basis of I_G. For every $f \in R[G]$ the multiplication

$$\mu_f \colon R[G] \to R[G], \quad \text{defined by } g \mapsto fg \quad \text{for every } g \in R[G]$$

is an R-module homomorphism.

Let M be a finitely generated R-module and $r \in \mathbbm{N}$. We say that M has *rank* r (and write $\mathrm{rk}(M) = r$) if the following two conditions are satisfied:

- If $(x_i)_{i \in I}$ is a free family in M, then $|I| \le r$.
- There is a free family $(x_i)_{i \in I}$ in M with $|I| = r$.

If $N \subset M$ is a submodule, then $\mathrm{rk}(M) \ge \mathrm{rk}(N) + \mathrm{rk}(M/N)$, and equality holds for integral domains (see [19, Korollar, page 113]). For an R-module homomorphism $\mu \colon M \to M$ let $\mathrm{rk}(\mu) = \mathrm{rk}\big(\mu(M)\big)$ denote the *rank of* f.

Let K be a field. We denote by $\mathrm{Hom}(G, K^\times)$ 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

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

For $n \in \mathbbm{N}$, let $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\} \subset K^\times$ denote the group of n-th roots of unity of K. $\mu_n(K)$ is a cyclic subgroup of $K^\times$. If $\exp(G) = n$, then $\mathrm{Hom}(G, K^\times) = \mathrm{Hom}(G, \mu_n(K))$, and K is called a *splitting field* of G if $|\mu_n(K)| = n$.

If K be a splitting field of G, then $\mathrm{char}(K) \nmid \exp(G)$, $|G| = |G|\,1_K \in K^\times$, $G \cong \mathrm{Hom}(G, K^\times)$, 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]).

Proposition 3.1. *Let G be a finite abelian group, $g \in G$, R an integral domain and $a \in R$.*

1. *$X^g - a \in R[G]$ is a zero-divisor if and only if $a^{\mathrm{ord}(g)} = 1$.*
2. *$\mathrm{rk}\big(\mu_{X^g - a}\big) \ge |G|\big(1 - \frac{1}{\mathrm{ord}(g)}\big)$.*

Proof. We set $m = \mathrm{ord}(g)$. If $g = 0$, then both assertions hold true. Suppose that $m \ge 2$.

1. There is some $f \in R[G]$ such that $(X^g)^m - a^m = (X^g - a)f$. If $a^m = 1$, then $(X^g)^m - a^m = X^0 - 1 = 0$ whence $X^g - a$ is a zero-divisor. If $a^m \neq 1$, then $(X^g)^m - a^m = 1 - a^m \in R \setminus \{0\} \subset K^\times \subset K[G]^\times$ where K is a quotient field of R. Thus $X^g - a$ is a unit in $K[G]$ whence it is not a zero-divisor in $R[G]$.

2. We set $M_1 = \langle (X^g - a)X^h \mid h \in G \rangle_R$ and have to verify that

$$\mathrm{rk}(M_1) \;\ge\; |G|\big(1 - \frac{1}{m}\big)\,.$$

Let $H = \langle g \rangle$, $\varphi = |G/H|$, $h_1, \ldots, h_\varphi \in G$ such that

$$G/H = \bigcup_{j=1}^{\varphi} (h_j + H)\,,$$

and let

$$M_2 = \langle X^{h_1}, \ldots, X^{h_\varphi} \rangle_R \quad \text{and} \quad M = M_1 + M_2 = \langle (X^g - a)X^h, X^{h_1}, \ldots, X^{h_\varphi} \mid h \in G \rangle_R\,.$$

We assert that $M = R[G]$. This implies that

$$\mathrm{rk}(M_1) \ge \mathrm{rk}\big(M_1/(M_1 \cap M_2)\big) = \mathrm{rk}\big((M_1 + M_2)/M_2\big) = \mathrm{rk}(R[G]) - \mathrm{rk}(M_2) = |G| - \varphi\,.$$

We have to show that $X^h \in M$ for every $h \in G$. Let $j \in [1, \varphi]$. It suffices to verify that

$$X^{h_j + lg} \in M \quad \text{for every} \quad l \in [0, m-1]\,.$$

For this we proceed by induction on l. If $l = 0$, then $X^{h_j} \in M$ by construction. Let $l > 0$ and suppose that $X^{(l-1)g+h_j} \in M$. Since $(X^g - a)X^{(l-1)g+h_j} \in M$, it follows that $X^{lg+h_j} \in M$. □

Proposition 3.2. *Let G be a finite abelian p-group, R an integral domain and $f \in R[G]$.*

1. *If $R = \mathbb{Z}$, K a field with $\mathrm{char}(K) = 0$ and $\chi\colon G \to K^\times$ a homomorphism with $\chi(f) = 0$, then $p \mid_{\mathbb{Z}} \varepsilon(f)$.*
2. *If $\mathrm{char}(R) = p$, then $f \in R[G]^\times$ if and only if $\varepsilon(f) \in R^\times$.*

Proof. We set $\exp(G) = n$ and

$$f = \sum_{g \in G} c_g X^g = \varepsilon(f) + \sum_{g \in G} c_g (X^g - 1)\,.$$

1. After enlarging K if necessary we may suppose that there is some $\zeta \in \mu_n(K) \subset K^\times$ with $\mathrm{ord}(\zeta) = n$. Then

$$0 = \chi(f) = \sum_{i=0}^{n-1} a_i \zeta^i\,, \quad \text{where} \quad a_i = \sum_{\substack{g \in G \\ \chi(g) = \zeta^i}} c_g \quad \text{for all} \quad i \in [0, n-1]\,,$$

and we set $P = a_{n-1}T^{n-1} + \ldots + a_0 \in \mathbb{Z}[T]$. Since $P(\zeta) = 0$, P is a multiple of the n-th cyclotomic polynomial Φ_n and hence we get $\Phi_n(1) \mid P(1)$. Since $\Phi_n(1) = p$ and

$$P(1) = \sum_{i=0}^{n-1} a_i = \sum_{g \in G} c_g = \varepsilon(f)\,,$$

the assertion follows.

2. If $g \in G$ and m is a power of p with $mg = 0$, then $(1 - X^g)^m = 1^m - X^{mg} = 0$. Thus we get $f^n = \varepsilon(f)^n$ whence $f \in R[G]^\times$ if and only if $\varepsilon(f) \in R[G]^\times \cap R = R^\times$. □

Proposition 3.3. *Let G be a finite abelian group, $l \in \mathbb{N}$, $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ a sequence over G, $k \in [1, l]$ and K a field.*

1. *For every subset $X \subset \mathrm{Hom}(G, K^\times)$ there exist $a_1, \ldots, a_k \in K^\times$ such that*

$$\big|\{\chi \in X \mid \chi(g_i) \ne a_i \ \text{ for all } \ i \in [1,k]\}\big| \ \le \ |X| \prod_{i=1}^{k} \Big(1 - \frac{1}{\mathrm{ord}(g_i)}\Big)\,.$$

2. *Let K be a splitting field of G and $a_1, \ldots, a_k \in K^\times$. If*

$$\big|\{\chi \in \mathrm{Hom}(G, K^\times) \mid \chi(g_i) \neq a_i \ \text{ for all } \ i \in [1,k]\}\big| \le l - k\,,$$

then there exist $a_{k+1}, \ldots, a_l \in K^\times$ such that

$$(X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) = 0\,.$$

Proof. See [16, Lemma 5.5.3 and Proposition 5.5.4]. □

Let G be a finite abelian group and R a commutative ring. Under varying assumptions on R, basic properties of the annihilator $\mathrm{Ann}(f)$, for elements $f \in R[G]$, are derived in the literature, mainly by lengthy explicit calculations. We give a unified proof of all these results in the setting of Artinian Gorenstein rings. Note, that the group algebra $R[G]$ is Artinian if and only if R is Artinian by Connell's Theorem (see [17, 20.7]). Furthermore, if R is a Gorenstein ring, then the same is true for the polynomial ring over R and the quotient ring

$$R/\langle a_1, \ldots, a_r\rangle_R \quad \text{for every regular sequence} \quad (a_1, \ldots, a_r)\,.$$

Thus, if R is a Gorenstein ring and $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$, then

$$R[G] \ \cong \ R[X_1, \ldots, X_r]/\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle_R$$

is a Gorenstein ring.

Proposition 3.4. *Let A be an Artinian Gorenstein ring and $x, y \in A$.*

1. $\mathrm{Ann}(x) \subset \mathrm{Ann}(y)$ *if and only if* $yA \subset xA$.
2. $\mathrm{Ann}(x) = \{0\}$ *if and only if* $x \in A^\times$.
3. $\mathrm{Ann}(x) = \mathrm{Ann}(y)$ *if and only if* $yA^\times = xA^\times$.

Proof. We need some basic properties of commutative Artinian rings (see [2, Chapter 8]). Since A is commutative Artinian, A is zero-dimensional and $A = A_1 \times \ldots \times A_n$ where $n \in \mathbb{N}$ and $A_1, \ldots, A_n$ are local Artinian rings. Since $A^\times = A_1^\times \times \ldots \times A_n^\times$ and, for every $z = (z_1, \ldots, z_n) \in A$, $\mathrm{Ann}_A(z) = \mathrm{Ann}_{A_1}(z_1) \times \ldots \times \mathrm{Ann}_{A_n}(z_n)$, we may suppose that A is local. Let $\mathfrak{m} = A \setminus A^\times$ denote its maximal ideal. Since $\mathfrak{m}$ is nilpotent, there is some $N \in \mathbb{N}$ such that $\mathfrak{m}^N = \{0\}$. Furthermore, since $\mathrm{Ann}(z) = A$ if and only if $z = 0$, we may suppose that $x, y \in A \setminus \{0\}$.

1. Suppose that $\mathrm{Ann}(x) \subset \mathrm{Ann}(y)$. Since A is a local Artinian Gorenstein ring, [4, 3.2.15] implies that

$$xA = \mathrm{Ann}\big(\mathrm{Ann}(x)\big) \supset \mathrm{Ann}\big(\mathrm{Ann}(y)\big) = yA\,.$$

Conversely, if $yA \subset xA$, say $y = xz$ for some $z \in A$, and $r \in \mathrm{Ann}(x)$, then $ry = rxz = 0$ whence $r \in \mathrm{Ann}(y)$.

2. If $\mathrm{Ann}(x) = \{0\}$, then $x^N \neq 0$ whence $x \in A \setminus \mathfrak{m} = A^\times$. Conversely, if $x \in A^\times$ and $r \in \mathrm{Ann}(x)$, then $rx = 0$ whence $r = rxx^{-1} = 0$.

3. Suppose that $\mathrm{Ann}(x) = \mathrm{Ann}(y)$. Then 1. implies that there are $\alpha, \beta \in A$ such that $x = \alpha y$ and $y = \beta x$. Then $x = \alpha\beta x$ and $(1 - \alpha\beta)x = 0$. Since $x \neq 0$, we obtain that $1 - \alpha\beta \notin A^\times$ whence $\alpha\beta \notin \mathfrak{m}$ and thus $\alpha, \beta \in A^\times$. Conversely, if $yA^\times = xA^\times$, then $yA = xA$ whence 1. implies that $\mathrm{Ann}(x) = \mathrm{Ann}(y)$. □

Corollary 3.5. *Let G be a finite abelian group, K a splitting field of G and $f \in K[G]$.*

1. *We have* $f \in K[G]^\times$ *if and only if* $\chi(f) \neq 0$ *for every* $\chi \in \mathrm{Hom}(G, K^\times)$.
2. *Suppose that* G *is a* p*-group,* $\mathbb{Z} \subset K$ *and* $f \in \mathbb{Z}[G]$. *If* $\varepsilon(f) \notin p\mathbb{Z}$, *then* $f \in K[G]^\times$.

Proof. 1. If $f \in K[G]^\times$, then obviously $\chi(f) \neq 0$ for every $\chi \in \mathrm{Hom}(G, K^\times)$. Conversely, suppose that $\chi(f) \neq 0$ for all $\chi \in \mathrm{Hom}(G, K^\times)$. By Proposition 3.4.2 it suffices to show that $\mathrm{Ann}(f) = \{0\}$. If $g \in \mathrm{Ann}(f)$, then $fg = 0$ whence $0 = \chi(f)\chi(g)$ for all $\chi \in \mathrm{Hom}(G, K^\times)$. This implies that $\chi(g) = 0$ for all $\chi \in \mathrm{Hom}(G, K^\times)$ and thus $g = 0$.

2. If $\varepsilon(f) \notin p\mathbb{Z}$, then Proposition 3.2.1 implies that $\chi(f) \neq 0$ for every $\chi \in \mathrm{Hom}(G, K^\times)$ whence the assertion follows from 1. □

4. Proof of Theorem 6.3 and of Corollary 1.2

Let K be a field and V a finite dimensional K-vector space. If $l \in \mathbb{N}$ and $f_1, \ldots, f_l \colon V \to V$ are K-linear, then

$$\mathrm{rk}(f_1 \circ \ldots \circ f_l) \geq \sum_{i=1}^{l} \mathrm{rk}(f_i) - (l-1)\dim(V)\,. \tag{4.1}$$

Proof of Theorem 6.3. Let $l \in \mathbb{N}$, R an integral domain with quotient field K and $a_1, \ldots, a_l \in R$, $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ and $f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_1} - a_l) \in R[G] \subset K[G]$. If p is the smallest prime divisor of $\exp(G)$ and $|S| < p$, then

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

Hence it suffices to suppose that $\mathsf{k}(S) < 1$ and to show that $f \neq 0$.

We have

$$f = f_1 \cdot \ldots \cdot f_l \quad \text{where} \quad f_i = X^{g_i} - a_i \quad \text{for every} \quad i \in [1, l]\,.$$

We consider the maps $\mu_f, \mu_{f_1}, \ldots, \mu_{f_l} \colon K[G] \to K[G]$ and show that $\mathrm{rk}(\mu_f) > 0$. This implies that $\mu_f \neq 0$ whence $f \neq 0$. Since $\mu_f = \mu_{f_1} \circ \ldots \circ \mu_{f_l}$ and $\dim K[G] = |G|$, Equation 4.1 and Proposition 3.1 imply that

$$\mathrm{rk}(\mu_f) \geq \sum_{i=1}^{l} \mathrm{rk}(\mu_{f_i}) - (l-1)|G| \geq l|G| - |G|\mathsf{k}(S) - (l-1)|G| = |G|\big(1 - \mathsf{k}(S)\big) > 0\,.$$

□

Proof of Corollary 1.2. (a) ⇒ (b) Assume to the contrary that there exists some $i \in [1, n-1]$ such that $\mathrm{ord}(g_i) < n$, say $i = 1$. We apply Proposition 3.3 with $l = n-1$ and $k = 1$. There exists some $a_1 \in K^\times$ such that

$$\big|\{\chi \in \mathrm{Hom}(G, K^\times) \mid \chi(g_i) \neq a_1\}\big| \leq |G|\Big(1 - \frac{1}{\mathrm{ord}(g_1)}\Big) \leq n\Big(1 - \frac{2}{n}\Big) \leq n - 2\,,$$

and there are $a_2, \ldots, a_{n-1} \in K^\times$ such that

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

a contradiction.

(b) $\Rightarrow$ (a) If $\ord(g_1) = \ldots = \ord(g_{n-1}) = n$, then $\mathsf k(S) < 1$ whence the assertion follows by Theorem 6.3. □

Next we provide the announced example of a sequence $S \in \mathcal F(G)$ of length $|S| = p+1$, where p is a prime divisor of $\exp(G)$, for which an associated element in a group algebra equals zero.

Example 4.1. Let G a finite abelian group, $g, h \in G$ two independent elements with $\ord(g) = \ord(h) = p$ for some odd prime p and

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

Then, for every commutative ring R, we have

$$f = (1 - X^g)(1 - X^h) \prod_{i=1}^{p-1} (1 - X^{g+ih}) = 0 \in R[G]\,.$$

Proof. We have

$$\begin{aligned} f &= (1 - X^h) \prod_{i=0}^{p-1} (1 - X^{g+ih}) \\ &= (1 - X^h)\Big(1 + \sum_{t=1}^{p} (-1)^t X^{tg} \sum_{0 \le i_1 < \ldots < i_t \le p-1} X^{i_1 h + \ldots + i_t h}\Big) \\ &= (1 - X^h)\Big(\sum_{t=1}^{p-1} (-1)^t X^{tg} \sum_{0 \le i_1 < \ldots < i_t \le p-1} X^{i_1 h + \ldots + i_t h}\Big)\,. \end{aligned}$$

Let $t \in [1, p-1]$. Since

$$(1 - X^h)(1 + X^h + \ldots + X^{(p-1)h}) = 1 - X^{ph} = 1 - X^0 = 0\,,$$

it suffices to verify that, for every $t \in [1, p-1]$,

$$\sum_{0 \le i_1 < \ldots < i_t \le p-1} X^{(i_1 + \ldots + i_t)h}$$

is a multiple of $1 + X^h + \ldots + X^{(p-1)h}$. Let $j \in [1, p-1]$. It is sufficient to prove that the number of solutions in $[0, p-1]$ of the congruence

$$(*) \qquad i_1 + \ldots + i_t \equiv j \mod p$$

equals the number of solutions of the congruence

$$(**) \qquad i_1 + \ldots + i_t \equiv 0 \mod p$$

Let $s \in [1, p-1]$ such that $st \equiv j \mod p$. If $(i_1, \ldots, i_t) \in [0, p-1]^t$ is a solution of $(*)$, then $(i_1 - s, i_2 - s, \ldots, i_t - s)$ is a solution of $(**)$. Conversely, if $(i_1, \ldots, i_t) \in [0, p-1]^t$ is a solution of $(**)$, then $(i_1 + s, \ldots, i_t + s)$ is a solution of $(*)$. □

5. Transversals of additive Latin squares

In this section we show how our main result on group algebras can be applied 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.

Let G be an additive abelian group and $l \in \mathbb{N}$. Characterize l-tuples $A = (g_1, \ldots, g_l)$ consisting of pairwise distinct elements of G which have the following property:

P(A) For every l-tuple $(h_1, \ldots, h_l)$ of elements in G, where repetition of elements is allowed, there is some permutation $\pi \in \mathfrak{S}_l$ such that the sums $g_1 + h_{\pi(1)}, \ldots, g_l + h_{\pi(l)}$ are pairwise distinct.

We say that l has Property **P** if every l-tuple $A = (g_1, \ldots, g_l)$ of pairwise distinct elements of G has Property **P**(A).

We start with some elementary remarks on these properties.

Suppose that G is torsionfree. Let $l \in \mathbb{N}$, and let $(g_1, \ldots, g_l)$ and $(h_1, \ldots, h_l)$ be l-tuples of elements in G where $g_1, \ldots, g_l$ are pairwise distinct. Since G can be totally ordered, there is some renumbering of the tuples such that $g_1 < \ldots < g_l$ and $h_1 \leq \ldots \leq h_l$ whence $g_1 + h_1 < \ldots < g_l + h_l$.

Suppose that G contains some non-zero torsion element $g \in G$, say $\mathrm{ord}(g) = n \in \mathbb{N}$. Then clearly there is no renumbering of the tuples $(0, g, 2g, \ldots, (n-1)g)$ and $(0, \ldots, 0, g)$ such that the associated sums are pairwise distinct. In particular, if G has some element of order 2, then the largest integer l satisfying Property **P** equals 1.

There is the following conjecture (see [6, Page 23]) and also [23, Conjecture 3]):

Conjecture: Let G be a finite abelian group of odd order and let p be the smallest prime divisor of $\exp(G)$. Then every $l < p$ satisfies Property **P**.

The Conjecture was first proved for prime cyclic groups by N. Alon (see [1]), and then for cyclic groups of prime power order and for elementary p-groups by S. Dasgupta et. al. (see [6, Theorem 2]). Theorem 6.3 and a crucial combinatorial lemma by S. Dasgupta offer a new approach to this problem which we present in Theorem 5.2 and in Corollary 5.3 (Statements 2. and 3. of the corollary were first obtained in [14]).

Let A be a commutative ring, $l \in \mathbb{N}$ and $\mathfrak{S}_l$ the group of permutations of a set with l elements. 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 matrix $M = (x_{i,j})_{1 \leq i,j \leq l} \in M_l(A)$ let

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

denote the permanent of M.

Proposition 5.1. *Let A be a commutative ring, $l \in \mathbb{N}$ and $x_1, \ldots, x_l, y_1, \ldots, y_l \in A$. If for every $\pi \in \mathfrak{S}_l$*

$$P_\pi = \prod_{1 \le i < j \le l} \big(x_j y_{\pi(j)} - x_i y_{\pi(i)}\big)\,,$$

then we have

$$\sum_{\pi \in \mathfrak{S}_l} P_\pi \;=\; \mathrm{Det}V(x_1, \ldots, x_l)\,\mathrm{Per}V(y_1, \ldots, y_l)\,.$$

Proof. This follows from [6, Lemma 5]. □

Theorem 5.2. *Let G be a finite abelian group of odd order, $l \in \mathbb{N}$, $(g_1, \ldots, g_l)$ an l-tuple of pairwise distinct elements of G and $(h_1, \ldots, h_l)$ an l-tuple of elements of G where repetition of elements is allowed. In each of the following cases there exists some permutation $\pi \in \mathfrak{S}_l$ such that the sums $g_1 + h_{\pi(1)}, \ldots, g_l + h_{\pi(l)}$ are pairwise distinct:*

1. *G is p-group, $l < p$, K a field with $\mathrm{char}(K) \in \{0, p\}$ and $\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l}) \neq 0 \in K[G]$.*
2. *G is cyclic, K a field with $\mathrm{char}(K) \nmid |G|$ and $\mathrm{Per}V(X^{h_1}, \ldots, X^{h_l}) \in K[G]^\times$.*
3. $$\sum_{1 \le i < j \le l} \Big(\frac{1}{\mathrm{ord}(g_j - g_i)} + \frac{1}{\mathrm{ord}(h_j - h_i)}\Big) < 1\,.$$

Proof. Let K be a field and $\widehat{G} = \mathrm{Hom}(G, K^\times)$. We intend to apply Proposition 5.1 with $A = K[G]$, $x_i = X^{g_i}$, $y_i = X^{h_i}$ for every $i \in [1, l]$, and we show that

$$\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l})\,\mathrm{Per}V(X^{h_1}, \ldots, X^{h_l}) \;\neq 0\,.$$

Then by Proposition 5.1 there exists some $\pi \in \mathfrak{S}_l$ such that

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

whence the sums $g_1 + h_{\pi(1)}, \ldots, g_l + h_{\pi(l)}$ are pairwise distinct.

1. We set
$$f = \mathrm{Per}V(X^{h_1}, \ldots, X^{h_l}) \;=\; \sum_{g \in G} b_g X^g\,,$$
and then, by the very definition of the permanent, we have
$$\varepsilon(f) = \sum_{g \in G} b_g \;=\; l! \;=\; l! \cdot 1_K \;\in\; K\,.$$

We distinguish two cases.

CASE 1: $\mathrm{char}(K) = p$.

Since $l < p$, it follows that $\varepsilon(f) \neq 0$. Then Proposition 3.2.2 implies that $f \in K[G]^\times$, and thus $f\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l}) \neq 0$.

CASE 2: $\mathrm{char}(K) = 0$.

Without restriction we may suppose that $\mathbb{Z} \subset K$ and that K is a splitting field of G. Since $l < p$, it follows that $\varepsilon(f) \notin p\mathbb{Z}$. Then Corollary 3.5.2 implies that $f \in K[G]^\times$, and thus $f\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l}) \neq 0$.

2. Without restriction we may suppose that K is a splitting field of G. For all $1 \leq i < j \leq l$ we have $X^{g_j - g_i} \neq 1$ whence

$$G_{i,j} = \{\chi \in \widehat{G} \mid \chi(X^{g_j - g_i}) = 1\}$$

is a proper subgroup of $\widehat{G}$. Since $\widehat{G} \cong G$ is cyclic, there is some

$$\chi \in \widehat{G} \setminus \bigcup_{1 \leq i < j \leq l} G_{i,j}$$

and then

$$\chi\Big(\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l})\Big) \neq 0\,.$$

Since $\mathrm{Per}V(X^{h_1}, \ldots, X^{h_l}) \in K[G]^\times$, it follows that

$$\chi\Big(\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l})\,\mathrm{Per}V(X^{h_1}, \ldots, X^{h_l})\Big) \neq 0$$

whence $\mathrm{Det}V(X^{g_1}, \ldots, X^{g_l})\,\mathrm{Per}V(X^{h_1}, \ldots, X^{h_l}) \neq 0$.

3. If K is a field with $\mathrm{char}(K) = 2$, then

$$\begin{aligned}
\mathrm{Det}V(X^{g_1}, \cdots, X^{g_l})\mathrm{Per}V(X^{h_1}, \cdots, X^{h_l}) &= \mathrm{Det}V(X^{g_1}, \cdots, X^{g_l})\mathrm{Det}V(X^{h_1}, \cdots, X^{h_l}) \\
&= \prod_{1 \leq i < j \leq l} (X^{g_j} - X^{g_i}) \prod_{1 \leq i < j \leq l} (X^{h_j} - X^{h_i}) \\
&= \prod_{1 \leq i < j \leq l} X^{g_i}(X^{g_j - g_i} - 1) \prod_{1 \leq i < j \leq l} X^{h_i}(X^{h_j - h_i} - 1) \\
&= u \prod_{1 \leq i < j \leq l} (X^{g_j - g_i} - 1)(X^{h_j - h_i} - 1) \neq 0\,,
\end{aligned}$$

where $u \in K[G]^\times$, and the last product is non-zero by Theorem 6.3. □

Corollary 5.3. *Let G be a finite abelian group of odd order, p the smallest prime divisor of $\exp(G)$, $l \in \mathbb{N}$, $(g_1, \ldots, g_l)$ an l-tuple of pairwise distinct elements of G and $(h_1, \ldots, h_l)$ an l-tuple of elements of G where repetition of elements is allowed. In each of the following cases there exists some permutation $\pi \in \mathfrak{S}_l$ such that the sums $g_1 + h_{\pi(1)}, \ldots, g_l + h_{\pi(l)}$ are pairwise distinct:*

1. *G is p-group, $l < p$ and $\sum_{1 \leq i < j \leq l} \Big(\frac{1}{\mathrm{ord}(g_j - g_i)}\Big) < 1$.*
2. *G is p-group and $l < \frac{1}{2} + \frac{1}{2}\sqrt{8p+1}$.*
3. *The elements $h_1, \ldots, h_l$ are pairwise distinct and $l < \frac{1}{2} + \frac{1}{2}\sqrt{4p+1}$.*

Proof. 1. We have

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

Since the first factor is a unit in $K[G]$, and the second factor is non-zero by Theorem 6.3, the assertion follows by Theorem 5.2.1.

2. Since

$$\sum_{1 \leq i < j \leq l} \Big(\frac{1}{\mathrm{ord}(g_j - g_i)}\Big) \leq \frac{1}{p}\binom{l}{2} < 1\,,$$

the assertion follows from 1.

3. Since $g_1, \ldots, g_l$ are pairwise distinct and $h_1, \ldots, h_l$ are pairwise distinct, it follows that

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

whence the assertion follows from Theorem 5.2.3. □

6. CAN WE GET A SHARP RESULT IN ALL CASES

1. Proposition 3.1: Für 1. benötigt man nicht, dass R ein Hauptidealring ist, und auch die wesentliche Aussage in 2., nämlich $M = R[G]$, gilt allgemein.

2. Theorem 1 wird nur schärfer, wenn man R vergrößert. Man verliert daher nichts, wenn man von vornherein R als Körper annimmt.

3. Die Proposition über artinsche Gorensteinringe kann ich auch nicht besser. Aber schießt man da nicht mit Kanonen auf Spatzen? Der Beweis von Corollary 3.5.1 läßt sich einfacher so bewerkstelligen. $K[G]$ ist eine nulldimensionale endlich erzeugte reduzierte K-Algebra.

There are natural bijections

$$\max(K[G]) \xleftarrow{\alpha} \operatorname{Hom}_{K-\mathrm{Alg}}(K[G], K) \xrightarrow{\beta} \operatorname{Hom}(G, K^\times),$$

given by $\alpha(\varphi) = \operatorname{Ker}(\varphi)$ and $\beta(\varphi) = \varphi \,|\, K$ (the surjectivity of α comes from the fact that K is a splitting field). Now

$$f \in K[G]^\times \iff f \text{ lies in no maximal ideal} \iff \chi(f) \neq 0 \text{ for all } \chi \in \operatorname{Hom}(G, K^\times)$$

Mit derselben Idee folgt auch:

$$f = 0 \iff f \text{ lies in every maximal ideal} \iff \chi(f) = 0 \text{ for all } \chi \in \operatorname{Hom}(G, K^\times)$$

Damit kann man sich in Example 4.1 die komplizierten Gruppenringrechnungen ersparen und (wahrscheinlich) für elementar-abelsche p-Gruppen ein etwas schärferes Resultat zeigen.

Lemma 6.1. *Let G be a finite abelian group, K a splitting field of G, $k \in \mathbb{N}$, $g_1, \ldots, g_k \in G$ independent elements, $a_1, \ldots, a_k \in K$ and $f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k)$. For $i \in [1,k]$ let $n_i = \operatorname{ord}(g_i)$ and*

$$\varepsilon_i = \begin{cases} 1\,, & \text{if} \quad a_i^{n_i} = 1\,, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\dim_K f\,K[G] \;\geq\; \big|\{\chi \in \widehat{G} \mid \chi(g_i) \neq a_i \;\text{ for all }\; i \in [1,k]\,\}\big| \;=\; |G| \prod_{i=1}^{k} \Big(1 - \frac{\varepsilon_i}{n_i}\Big)\,.$$

Proof. Let $V = \{\lambda \in K[G] \mid f\lambda = 0\}$ and $\Omega = \{\chi \in \widehat{G} \mid \chi(f) \neq 0\}$. If $\lambda \in V$, then $\chi(\lambda) = 0$ for all $\chi \in \Omega$ and therefore $\dim_K V \leq |G| - |\Omega|$, whence $\dim_K fK[G] \geq |\Omega|$. Clearly, $\Omega = \{\chi \in \widehat{G} \mid \chi(g_i) \neq a_i \text{ for all } i \in [1,k]\,\}$.

Let $G_0 = \langle g_1, \ldots, g_k \rangle$. Then $\widehat{G_0} = \langle \chi_1, \ldots, \chi_k \rangle$, where

$$\chi_i(g_j) = \begin{cases} 1\,, & \text{if} \quad i \neq j\,, \\ \zeta_{n_j}\,, & \text{if} \quad i = j\,, \end{cases}$$

and $\zeta_{n_j} \in K$ denotes a primitive n_j-th root of unity. For $i \in [1,k]$ and $a_i^{n_i} = 1$, let $d_i \in [1, n_i]$ with $a_i = \zeta_{n_i}^{d_i}$. Now let $\chi = \chi_1^{t_1} \cdot \ldots \cdot \chi_k^{t_k} \in \widehat{G_0}$ with $t_i \in [1, n_i]$ for all $i \in [1,k]$. Then we have

$\chi(g_i) \neq a_i$ for all $i \in [1,k]$ if and only if $t_i \neq d_i$ for all $i \in [1,t]$ with $\varepsilon_i = 1$. Now every $\chi \in \widehat{G_0}$ has $|G|/|G_0|$ extensions to a character of G, and therefore

$$|\Omega| \ = \ \frac{|G|}{|G_0|} \prod_{i=1}^{k} (n_i - \varepsilon_i) \ = \ |G| \prod_{i=1}^{k} \Big(1 - \frac{\varepsilon_i}{n_i}\Big) \, .$$

□

Theorem 6.2. *Let G be a finite abelian group, K a splitting field of G, $l \in \mathbbm{N}$, $k \in [1,l]$, 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 $n_i = \mathrm{ord}(g_i)$ and suppose that*

$$\sum_{i=1}^{l} \frac{1}{n_i} \ - \ \sum_{i=2}^{k} (-1)^i \sum_{1 \le \nu_1 < \ldots < \nu_i \le k} \frac{1}{n_i} \ < \ 1 \, .$$

Then

$$\prod_{i=1}^{l} (X^{g_i} - a_i) \ \neq \ 0 \quad \text{for all} \quad a_1, \ldots, a_k \in K \, .$$

Remark. If $S = g_1 \cdot \ldots \cdot g_l$, then the assumption of the Theorem holds if either $\mathsf k(S) < 1$ or $k \ge 2$ and $\mathsf k(S) \le 1$.

Proof. Let $f = (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_k} - a_k)$ and $f_i = (X^{g_i} - a_i)$ for $i \in [k+1, l]$. Then by (4.1) and the Lemma

$$\begin{aligned}
\dim_K f_{k+1} \cdot \ldots \cdot f_l \, f \, K[G] \ &\ge \ \dim_K f \, K[G] \ + \ \sum_{i=k+1}^{l} \dim_K f_i K[G] \ - \ (l-k)|G| \\
&\ge \ |G| \prod_{i=1}^{k} \Big(1 - \frac{1}{n_i}\Big) + \sum_{i=k+1}^{l} |G| \Big(1 - \frac{1}{n_i}\Big) - (l-k)|G| \\
&= \ |G| \Big[\prod_{i=1}^{k} \Big(1 - \frac{1}{n_i}\Big) - \sum_{i=k+1}^{l} \frac{1}{n_i} \Big] \ = \ |G| \Big[1 - \sum_{i=1}^{l} \frac{1}{n_i} + \sum_{i=2}^{k} (-1)^i \sum_{1 \le \nu_1 < \ldots < \nu_i \le k} \frac{1}{n_i} \Big] \ > 0
\end{aligned}$$

and therefore $f f_{k+1} \cdot \ldots \cdot f_l \neq 0$. □

Theorem 6.3. *Let G be a finite abelian group, $l \in \mathbb{N}$, $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ a sequence over G with $\langle \mathrm{supp}(S) \rangle = G$, $\mathsf{k}(S) = \mathrm{ord}(g_1)^{-1} + \ldots + \mathrm{ord}(g_l)^{-1}$ its cross number and R an integral domain. We say that $(*)$ holds if*

$$f \;=\; (X^{g_1} - a_1) \cdot \ldots \cdot (X^{g_l} - a_l) \neq 0 \in R[G] \quad \textit{for all} \quad a_1, \ldots, a_l \in R\,.$$

1. $\mathrm{char}(R) \nmid |G|$ *and* $\mathrm{supp}(S)$ *contains two independent elements. If* $\mathsf{k}(S) \le 1$*, then* $(*)$ *holds. This result is best possible as Example 4.1 shows.*
2. $\mathrm{char}(R) \nmid |G|$ *and each two elements of* $\mathrm{supp}(S)$ *are dependent.*
3. $\mathrm{char}(R) \mid |G|$ *and* $\mathrm{supp}(S)$ *contains two independent elements.*
4. $\mathrm{char}(R) \mid |G|$ *and each two elements of* $\mathrm{supp}(S)$ *are dependent.*

Is the above case distinction the right one ? do we have sharp results in all cases ??

Proof. 1.

2.

3. and 4. if $\mathrm{char}(R) = p$, then of course $(X^g - 1)^p = 0$. □

References

[1] N. Alon, *Additive Latin transversals*, Isr. J. Math. **117** (2000), 125 – 130.
[2] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.
[3] 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.
[4] W. Bruns and J. Herzog, *Cohen-Macaulay Rings rev. ed.*, Cambridge Univ. Press, 1998.
[5] S.T. Chapman, M. Freeze, W. Gao, and W.W. Smith, *On Davenport's constant of finite abelian groups*, Far East J. Math. Sci. **2** (2002), 47 – 54.
[6] S. Dasgupta, G. Károlyi, O. Serra, and B. Szegedy, *Transversals of additive Latin squares*, Isr. J. Math. **126** (2001), 17 – 28.
[7] S. Elledge and G.H. Hurlbert, *An application of graph pebbling to zero-sum sequences in abelian groups*, Integers **5(1)** (2005), Paper A17, 10p.
[8] P. van Emde Boas, *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam, 1969.
[9] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups III*, Reports ZW-1969-008, Math. Centre, Amsterdam, 1969.
[10] W. Gao, *Addition theorems and group rings*, J. Comb. Theory, Ser. A **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 Mt. J. Math., to appear.
[12] ———, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math., to appear.
[13] ———, *Zero-sum problems and coverings by proper cosets*, Eur. J. Comb. **24** (2003), 531 – 549.
[14] W. Gao and D.J. Wang, *Additive Latin transversals and group rings*, Isr. 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 and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
[17] R. Gilmer, *Commutative Semigroup Rings*, The University of Chicago Press, 1984.
[18] C.P. Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.
[19] E. Oeljeklaus and R. Remmert, *Lineare Algebra I*, Springer, 1974.
[20] J.E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8 – 10.
[21] C. Peng, *Addition theorems in elementary abelian groups I*, J. Number Theory **27** (1987), 46 – 57.
[22] ———, *Addition theorems in elementary abelian groups II*, J. Number Theory **27** (1987), 58 – 62.
[23] H.S. Snevily, *Unsolved problems: the Cayley addition table of* $\mathbb{Z}_n$, Am. Math. Mon. **106** (1999), 584 – 585.
[24] Zhi-Wei Sun, *On Snevily's conjecture and restricted sumsets*, J. Comb. Theory, Ser. A **103** (2003), 291 – 304.

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

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