European Journal of Combinatorics 41 (2014) 68–78

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Permutations over cyclic groups[☆]

Zoltán Lóránt Nagy

Department of Computer Science, Eötvös Loránd University, Budapest H-1117, Pázmány Péter sétány 1/C, Hungary

ARTICLE INFO

Article history:
Received 7 September 2011
Accepted 18 March 2014
Available online 16 April 2014

ABSTRACT

Generalizing a result in the theory of finite fields we prove that, apart from a couple of exceptions that can be classified, for any elements $a_1, \ldots, a_m$ of the cyclic group of order m, there is a permutation π such that $1a_{\pi(1)} + \cdots + ma_{\pi(m)} = 0$.

1. Introduction

The starting point of the present paper is the following result of Gács, Héger, Nagy and Pálvölgyi.

Theorem 1.1 ([7]). *Let $\{a_1, a_2, \ldots, a_p\}$ be a multiset in the finite field $GF(p)$, p a prime. Then after a suitable permutation of the indices, either $\sum_i ia_i = 0$, or $a_1 = a_2 = \cdots = a_{p-2} = a$, $a_{p-1} = a+b$, $a_p = a - b$ for field elements a and b, $b \neq 0$.*

A similar result using a slightly different terminology was obtained by Vinatier [10] under the extra assumption that $a_1, \ldots, a_p$, when considered as nonnegative integers, satisfy $a_1 + \cdots + a_p = p$. The former result can be extended to arbitrary finite fields in the following sense.

Theorem 1.2 ([7]). *Let $\{a_1, a_2, \ldots, a_q\}$ be a multiset in the finite field $GF(q)$, where q is a prime power. There are no distinct field elements $b_1, b_2, \ldots, b_q$ such that $\sum_i a_ib_i = 0$ if and only if after a suitable permutation of the indices, $a_1 = a_2 = \cdots = a_{q-2} = a$, $a_{q-1} = a + b$, $a_q = a - b$ for some field elements a and b, $b \neq 0$.*

This theorem can be reformulated in the language of finite geometry and also has an application about the range of polynomials over finite fields. For more details, see [7].

Our aim is to find a different kind of generalization, more combinatorial in nature, which refers only to the group structure. First we extend the result to cyclic groups of odd order.

☆ This research was supported by Hungarian National Scientific Research Funds (OTKA) grant 81310.
E-mail addresses: nagyzoltanlorant@gmail.com, nagyzoli@cs.elte.hu.

http://dx.doi.org/10.1016/j.ejc.2014.03.010
0195-6698/

Theorem 1.3. *Let $\{a_1, a_2, \dots, a_m\}$ be a multiset in the Abelian group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, where m is odd. Then after a suitable permutation of the indices, either $\sum_i ia_i = 0$, or $a_1 = a_2 = \dots = a_{m-2} = a$, $a_{m-1} = a + b$, $a_m = a - b$ for elements a and b, $(b, m) = 1$.*

The situation is somewhat different if the order of the group is even. In this case we have to deal with two types of exceptional structures. The following statements are easy to check.

Proposition 1.4. *Let m be an even number represented as $m = 2^k n$, where n is odd.*

(i) *If a multiset $M = \{a_1, a_2, \dots, a_m\}$ of $\mathbb{Z}_m$ consists of elements having the same odd residue c mod 2^k, then M has no permutation for which $\sum_i ia_i = 0$ holds.*
(ii) *If $M = \{a, a, \dots, a + b, a - b\}$ mod m, where a is even and $(b, m) = 1$ holds, then M has no permutation for which $\sum_i ia_i = 0$ holds.*

These two different kind of structures we call homogeneous and inhomogeneous exceptional multisets, respectively.

Theorem 1.5. *Let $M = \{a_1, a_2, \dots, a_m\}$ be a multiset in the Abelian group $\mathbb{Z}_m$, m even. If M is not an exceptional multiset as defined in Proposition 1.4, then after a suitable permutation of the indices $\sum_i ia_i = 0$ holds.*

The presented results might be extended in different directions. One may ask whether there exists a permutation of the elements of a given multiset M of $\mathbb{Z}_m$ (consisting of m elements), for which the sum $\sum_i ia_i$ is equal to a prescribed element of $\mathbb{Z}_m$. This question is related to a conjecture of Britnell and Wildon, see [4, p. 20], which can be reformulated as follows. Given a multiset $M = \{a_1, a_2, \dots, a_m\}$ of $\mathbb{Z}_m$, all elements of $\mathbb{Z}_m$ are admitted as the value of the sum $\sum_{i=1}^{m} ia_{\pi(i)}$ for an appropriate permutation π from the symmetric group Sym_m, unless one of the following holds:

- $M = \{a, \dots, a, a + b, a - b\}$,
- there exists a prime divisor p of m such that all elements of M are the same mod p.

Our result may in fact be considered as a major step towards the proof of their conjecture, which would provide a classification of values of determinants associated to special types of matrices. When m is a prime, the conjecture is an immediate consequence of Theorem 1.1 and Lemma 2.2(ii). Indeed, if only one value was admitted, then the multiset would consist of a single element m times. On the other hand, if there was an admitted element $w \neq 0$, all nonzero elements would be admitted via Lemma 2.2(ii). Thus the value 0 is the crucial one, which was investigated in Theorem 1.1.

As for another direction, these questions are also meaningful for arbitrary finite Abelian groups, but to find the exact characterization appears to be a difficult task in general. For example, in the Klein group $\mathbb{Z}_2^2$, the multiset consisting of all different group elements has no zero 'permutational sum', whereas all other multisets do have. Meanwhile in the group $\mathbb{Z}_2^3$, all multisets have a permutational sum which is zero.

As it was briefly explained in [7], the problem has a connection to Snevily's conjecture [9], solved recently by Arsovski [3], namely the following one. Given an Abelian group G of odd order m. Subsets $\{a_1, \dots, a_l\}$ and $\{b_1, \dots, b_l\}$ of G are also given, where $l \leq m$. Does there exist a permutation π in the symmetric group Sym_l such that $a_1 + b_{\pi(1)}, \dots, a_l + b_{\pi(l)}$ are pairwise distinct? It would be natural to try to adapt the techniques which were successful for Snevily's problem, but our problems are apparently more difficult. In order to prove Theorems 1.1 and 1.2, we had to replace the relatively simple approach of Alon [2] by a more delicate application of the Combinatorial Nullstellensatz [1,8] and we do not see how Theorem 1.3, for example, could be obtained by the method of [5].

The paper is organized as follows. In Section 2, we collect several simple observations that are used frequently throughout the paper and sketch our proof strategy. Section 3 is devoted to the proof of Theorem 1.3. In Section 4 we will verify Theorem 1.5 for some particular cases, whose proofs do not exactly fit in the general framework (and may be skipped at a first reading). The complete proof, which is more or less parallel to that of Theorem 1.3, is carried out in Section 5.