REMARKS TO ARSOVSKI'S PROOF OF SNEVILY'S CONJECTURE

Dedicated to our late friend, András Gács

GERGELY HARCOS[1] Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest, H–1364 Hungary
GYULA KÁROLYI[2] Institute of Mathematics, Eötvös University, Pázmány P. sétány 1/C, Budapest, H–1117 Hungary
GÉZA KÓS Institute of Mathematics, Eötvös University, Pázmány P. sétány 1/C, Budapest, H–1117 Hungary, and Computer and Automation Research Institute, Kende utca 13-17, Budapest, H–1111 Hungary

Abstract. Let G denote a finite Abelian group, and $\mathbb{F}$ a field whose multiplicative group $\mathbb{F}^\times$ contains an element whose order equals the exponent of G. For any pair $A = \{a_1, \ldots, a_k\}$, $B = \{b_1, \ldots, b_k\}$ of k-element subsets of G there exist homomorphisms $\chi_1, \ldots, \chi_k : G \to \mathbb{F}^\times$ such that neither of the two matrices $(\chi_i(a_j))$ and $(\chi_i(b_j))$ is singular. This confirms a conjecture of Feng, Sun, and Xiang. We also give a shortened proof of Snevily's conjecture.

1. Introduction

Let G denote a finite Abelian group of order m and exponent n. We say that G is *fully representable* over a field $\mathbb{F}$ if its multiplicative group $\mathbb{F}^\times$ contains an element of order n. This happens if and only if the characteristic of the field $\mathbb{F}$

[1] Supported by European Community Grant ERG 239277 and OTKA Grants K 72731 and PD 75126.
[2] Supported by Bolyai Research Fellowship and OTKA Grants K 67676 and NK 67867.

does not divide n, and $\mathbb{F}$ itself contains the splitting field of the polynomial $x^n - 1$ over its prime field. In this case $\mathbb{F}^\times$ contains a unique cyclic subgroup H of order n that may be identified for every such field of the same characteristic, and every homomorphism from G to $\mathbb{F}^\times$ maps into H. Such group characters with respect to pointwise multiplication form the character group $\widehat{G} \cong G$. It follows from the orthogonality relations

$$\sum_{g \in G} \chi_1(g)\chi_2^{-1}(g) = \begin{cases} |G| & \text{if } \chi_1 = \chi_2 \\ 0 & \text{otherwise} \end{cases}$$

that the $m \times m$ matrix $(\chi(g))_{g \in G, \chi \in \widehat{G}}$ is nonsingular. Thus, the characters are linearly independent over $\mathbb{F}$ and form a basis in the vector space of all $G \to \mathbb{F}$ functions over $\mathbb{F}$.

Remark. The independence of the columns of the character table can be interpreted as follows: For any subset $A = \{a_1, \ldots, a_k\}$ of G, those sets of characters χ for which the vectors $\chi(A) = \chi(a_i)_{1 \le i \le k}$ are independent over $\mathbb{F}$, form a rank k matroid $\mathcal{M}_A$ over the ground set $\widehat{G}$. Here we prove that for any two sets $A, B \subseteq G$ of the same cardinality, the matroids $\mathcal{M}_A$ and $\mathcal{M}_B$ have a common basis.

Theorem 1. *Assume that the finite Abelian group G is fully representable over the field $\mathbb{F}$. For any two subsets $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ of G there exist characters $\chi_1, \ldots, \chi_k \in \widehat{G}$ such that both $\operatorname{Det}(\chi_i(a_j))$ and $\operatorname{Det}(\chi_i(b_j))$ are different from zero.*

This confirms a conjecture of Feng, Sun, and Xiang [4]. Applying the natural isomorphism between G and $\widehat{\widehat{G}}$, one obtains the following dual version.

Theorem 2. *Under the conditions of the previous theorem, let $\mathrm{X} = \{\chi_1, \ldots, \chi_k\}$ and $\Psi = \{\psi_1, \ldots, \psi_k\}$ be two subsets of $\widehat{G}$. Then there exist elements $a_1, \ldots, a_k \in G$ such that both $\operatorname{Det}(\chi_i(a_j))$ and $\operatorname{Det}(\psi_i(a_j))$ are different from zero.*

Using the exterior algebra method, Feng, Sun, and Xiang [4] pointed out that a weaker form of Theorem 1 would imply Snevily's conjecture [6], which after a series of partially successful attempts [1, 3, 5], see also [7, 8], was recently proved by Arsovski [2]. Thus, one obtains the following affirmative answer for Snevily's problem.

Theorem 3. *Let G be an Abelian group of odd order. For any two subsets $A = \{a_1, \dots, a_k\}$ and $B = \{b_1, \dots, b_k\}$ of G there exists a permutation $\pi \in S_k$ such that the elements $a_1 + b_{\pi(1)}, \dots, a_k + b_{\pi(k)}$ are pairwise different.*

The proof of Theorem 1, at least for finite fields $\mathbb{F}$ of characteristic 2, is implicit in Arsovski's paper. Here we present a variant of his argument with considerable simplifications, which completely settles the conjecture of Feng, Sun, and Xiang.

2. The Proofs

Assume that, for a given finite Abelian group G, the statement of Theorem 1 fails for a certain field $\mathbb{F}$ of characteristic c, then it also fails for every field of characteristic c over which G is fully representable. In particular, it fails for the purely transcendental extension $\mathbb{F}' = \mathbb{F}(t_1, \dots, t_m)$. Accordingly, let $A = \{a_1, \dots, a_k\}$ and $B = \{b_1, \dots, b_k\}$ be two subsets of G such that

$$\mathrm{Det}(\chi_i(a_j))\,\mathrm{Det}(\chi_i(b_j)) = 0$$

holds for every k-tuple of characters $\chi_1, \dots, \chi_k \in \widehat{G}$. Write $\widehat{G} = \{\chi_1, \dots, \chi_m\}$. Let φ denote an arbitrary function from G to $\mathbb{F}'$; it can be uniquely expressed as $\varphi = \sum_{u=1}^{m} \lambda_u \chi_u$ with Fourier-coefficients $\lambda_u \in \mathbb{F}'$. Consider the $k \times m$ matrices $M = (m_{iu})$ and $N = (n_{iu})$ with $m_{iu} = \lambda_u \chi_u(a_i)$, resp. $n_{iu} = \chi_u(b_i)$. In view of the Cauchy–Binet formula and the multilinearity of the determinant, for the $k \times k$ matrix L with (i, j) entry $\varphi(a_i + b_j)$ we obtain

$$\begin{aligned}
\mathrm{Det}\,L &= \mathrm{Det}\Big(\sum_{u=1}^{m} \lambda_u \chi_u(a_i + b_j)\Big) = \mathrm{Det}\Big(\sum_{u=1}^{m} \lambda_u \chi_u(a_i)\chi_u(b_j)\Big) \\
&= \mathrm{Det}(MN^\top) = \sum_{1 \le u_1 < \cdots < u_k \le m} \mathrm{Det}(m_{iu_j})\,\mathrm{Det}(n_{iu_j}) \\
&= \sum_{1 \le u_1 < \cdots < u_k \le m} (\lambda_{u_1} \cdots \lambda_{u_k})\,\mathrm{Det}(\chi_{u_i}(a_j))\,\mathrm{Det}(\chi_{u_i}(b_j)) \\
&= 0.
\end{aligned}$$

Enumerate the elements of G as $g_1, \dots, g_m$, and apply the above formula for the function φ that maps each g_i to the corresponding t_i. Then $\mathrm{Det}\,L$ is the alternating sum of $k!$ monomial terms in $t_1, \dots, t_m$, each of degree k. Because of the algebraic independence of the elements t_i, $\mathrm{Det}\,L$ can only vanish if each monomial term cancels out, either because it appears with both $+$ and $-$ signs, or because it appears at least c times with the same sign. Anyway, for any permutation $\pi \in S_k$ there exists a permutation $\sigma \neq \pi \in S_k$ such that the elements $a_1 + b_{\sigma(1)}, \dots, a_k + b_{\sigma(k)}$, in some order, coincide with the elements $a_1 + b_{\pi(1)}, \dots, a_k + b_{\pi(k)}$. According to the following simple combinatorial lemma inherent in [2], this is impossible.

Lemma 4. *Let $A = \{a_1, \dots, a_k\}$ and $B = \{b_1, \dots, b_k\}$ be subsets of an arbitrary Abelian group G. There exists a permutation $\pi \in S_k$ such that for any permutation $\sigma \neq \pi \in S_k$, the multisets $\{a_1 + b_{\pi(1)}, \dots, a_k + b_{\pi(k)}\}$ and $\{a_1 + b_{\sigma(1)}, \dots, a_k + b_{\sigma(k)}\}$ are different.*

Proof. Fix the positive integer k, and assume that the lemma has already been verified for smaller values of k. Write $a_1 + b_1 = g$, and consider the set I of all indices i for which there exists an index j with $a_i + b_j = g$. We may assume that $I = \{1, \dots, \ell\}$. In the case $\ell = k$ there is a unique permutation π with $a_1 + b_{\pi(1)} = \dots = a_k + b_{\pi(k)} = g$. If $1 \leq \ell < k$, then fix the first ℓ values of π by $a_1 + b_{\pi(1)} = \dots = a_\ell + b_{\pi(\ell)} = g$, and apply the induction hypothesis for the multisets $A' = \{a_{\ell+1}, \dots, a_k\}$, $B' = \{b_i \mid i \neq \pi(1), \dots, \pi(\ell)\}$ to extend it to a permutation $\pi \in S_k$. □

This contradiction proves Theorem 1. Theorem 3 follows by the sophisticated argument of [4] or by the elegant reasoning of Arsovski [2]. In retrospect, the proof only relies on the identity (valid in characteristic 2)

$$\operatorname{Det}(\varphi(a_i + b_j)) = \sum_{1 \leq u_1 < \dots < u_k \leq m} \sum_{\pi \in S_k} \operatorname{Det}(\lambda_{u_j} \chi_{u_j}(a_i + b_{\pi(i)}))$$

and the existence of $\varphi = \sum_{u=1}^m \lambda_u \chi_u : G \to \mathbb{F}'$, guaranteed by Lemma 4, for which the left hand side is nonzero. Indeed, if Theorem 3 fails then each determinant on the right hand side is zero because the underlying matrix has two equal rows. The indentity can be proved directly using the multilinearity of the determinant and the multiplicativity of the characters χ_u:

$$\begin{aligned}
\operatorname{Det}(\varphi(a_i + b_j)) &= \sum_{1 \leq u_1, \dots, u_k \leq m} \operatorname{Det}(\lambda_{u_i} \chi_{u_i}(a_i + b_j)) \\
&= \sum_{\substack{1 \leq u_1, \dots, u_k \leq m \\ \text{distinct}}} \operatorname{Det}(\lambda_{u_i} \chi_{u_i}(a_i + b_j)) \\
&= \sum_{\substack{1 \leq u_1, \dots, u_k \leq m \\ \text{distinct}}} \sum_{\pi \in S_k} \prod_{i=1}^k (\lambda_{u_i} \chi_{u_i}(a_i + b_{\pi(i)})) \\
&= \sum_{1 \leq u_1 < \dots < u_k \leq m} \sum_{\pi \in S_k} \operatorname{Det}(\lambda_{u_j} \chi_{u_j}(a_i + b_{\pi(i)})).
\end{aligned}$$

It would be very interesting to find a purely combinatorial proof.

Acknowledgement. We are grateful to András Biró, András Frank, Péter Pál Pálfy and Csaba Szabó for discussions over this topic.

References

[1] N. Alon, Additive Latin transversals, *Israel J. Math.* **117** (2000) 125–130
[2] B. Arsovski, A proof of Snevily's conjecture, *Israel J. Math.*, to appear
[3] S. Dasgupta, Gy. Károlyi, O. Serra, and B. Szegedy, Transversals of additive Latin squares, *Israel J. Math.* **126** (2001) 17–28
[4] T. Feng, Z.W.Sun, and Q. Xiang, Exterior algebras and two conjectures on finite Abelian groups, *Israel J. Math.*, to appear
[5] W.D. Gao and D.J. Wang, Additive Latin transversals and group rings, *Israel J. Math.* **140** (2004) 375–380
[6] H. Snevily, The Cayley addition table of Z_n, *Amer. Math. Monthly* **106** (1999) 584–585
[7] Z.W. Sun, On Snevily's conjecture and restricted sumsets, *J. Combin. Th. A* **103** (2003) 291–304
[8] T. Tao and V.H. Vu, Additive Combinatorics, Cambridge University Press, 2006

E-mail address: gharcos@renyi.hu
E-mail address: karolyi@cs.elte.hu
E-mail address: kosgeza@cs.elte.hu