

CONDITIONS FOR MATCHABILITY IN GROUPS AND FIELD EXTENSIONS II

MOHSEN ALIABADI

Department of Mathematics
University of California
San Diego, 9500 Gilman Dr, La Jolla, Ca 92093, USA
e-mail: maliabadisr@ucsd.edu

Abstract

We present sufficient conditions for the existence of matchings in abelian groups and their linear counterparts. These conditions lead to extensions of existing results in matching theory. Additionally, we classify subsets within abelian groups that cannot be matched. We introduce the concept of Chowla subspaces and formulate and conjecture a linear analogue of a result originally attributed to Hamidoune [21] concerning Chowla subsets. If proven true, this result would extend matchings in primitive subspaces. Throughout the paper, we emphasize the analogy between matchings in abelian groups and field extensions. We also pose numerous open questions for future research. Our approach relies on classical theorems in group theory, additive number theory and linear algebra. As the title of the paper suggests, this work is the second sequel to a previous paper [5] with a similar theme. The paper is self-contained and can be read independently.

Keywords: Chowla subset, matchable subsets, matching property, Sidon subset.

2020 Mathematics Subject Classification: Primary: 05D15; Secondary: 11B75; 12F10.

1. INTRODUCTION

Let A and B be finite subsets of the multiplicative abelian group G with the same cardinality. A *matching* from A to B is a bijection $f : A \rightarrow B$ such that $af(a) \notin A$, for every $a \in A$. In this case, we say A is *matched* (or *matchable*) to B . The notion of matchings in abelian groups was initially introduced in [18] in order to generalize a geometric property of lattices in Euclidean space. Their goal was to demonstrate that a suitably selected fixed set of monomials,

if sufficiently small, could be removed from a generic homogeneous polynomial through a suitable linear change of coordinates. The inquiry into sets of removable monomials from generic homogeneous polynomials via linear transformations has historical origins dating back to [30]. Matchings have been extensively studied in the context of abelian groups [7, 26] as well as in arbitrary group settings [16]. The linear version of matchings is introduced in [17] and further investigated in [2, 4]. A matroidal analogue of matchings is introduced and explored in [6]. For enumerative aspects of matchings, see [21]. There are still many fascinating open problems in this area. This paper continues to study some problems motivated in [2, 5].

Evidently, it is necessary for the existence of a matching from A to B that $|A| = |B|$ and that $e \notin B$ (here e denotes the neutral element of G). One says that a group G possesses the *matching property* if these necessary conditions are sufficient as well. It is shown in [26] that an abelian group satisfies the matching property if and only if it is either torsion-free or cyclic of prime order. In [2], it is observed that the existence of a nontrivial proper finite subgroup serves as an obstruction to the matching property in general abelian groups. In particular, the following result is established in [2].

Theorem 1. *Let G be an abelian group and A be a finite subset of G which does not contain any coset of any proper nontrivial finite subgroup of G . Then for every finite subset B of G with $|A| = |B|$ and $e \notin B$, there is a matching from A to B .*

Theorem 1 was primarily established using methods from additive number theory and combinatorics. Specifically, it relied on Kneser's addition theorem (Theorem 8) in conjunction with Hall's Marriage Theorem. These theorems served as the key components in the classification of the matching property. Initially, they were employed in [26] and later adapted in [2] to prove Theorem 1.

In this paper, we first present additional sufficient conditions for the existence of matchings in abelian groups, wherein structures from additive number theory, such as Kemperman's structure theorem and Sidon subsets play prominent roles. In continuation of Theorem 1.1 in [5], where unmatchable subsets in the group setting are addressed. Our main results concerning matchable subsets appear as Theorems 2 and 3. All the necessary definitions and concepts from additive number theory are provided in Section 2. Note that in Theorem 2, $p(G)$ stands for the smallest cardinality of a nontrivial subgroup of G . If G is finite, then $p(G)$ equals the smallest prime divisor of $|G|$. On the other hand, $p(G) = \infty$ if and only if G is torsion free.

Theorem 2. *Let G be any abelian group, A and B be finite subsets of G with the same cardinality n and $e \notin B$. Assume further that one of the following conditions holds:*

1. $B \cap H = \emptyset$, for every proper finite subgroup H of G .
2. A and B are not contained in a union of l cosets of any nontrivial proper finite subgroup of G and $l \geq n - 1$.
3. A and B are not contained in a union of l cosets of any nontrivial proper finite subgroup of G , $l \geq n - 2$, $|\{a^n | a \in A\}| > 2$ and B has at least two elements whose orders are greater than n .
4. $p(G) = n$, and A is not a coset of any nontrivial subgroup of G .
5. A is a Sidon subset.
6. The order of every element of B is greater than or equal to n and A is not a progression.
7. For every nontrivial finite subgroup H of G and elements $a, b \in G$, $|aH \cap A| + |bH \cap B| < |H| + 1$.

Then A is matched to B .

In the following theorem, we establish that if A is not matched to B , then certain additive number-theoretical structures must exist within A .

Theorem 3. *Let A be a nonempty finite subset of an abelian group G . Assume that there exists a subset B of G with $|B| = |A|$ and $e \notin B$ so that A is not matched to B . Then one of the following conditions holds:*

- (i) A contains a progression;
- (ii) A contains a quasi-periodic subset.

We now turn our attention to linear matchings. Given a field extension $K \subset L$, an analogous notion of matchings between two K -subspaces of L is introduced and developed in [17].

Definition. Let A and B be two n -dimensional K -subspaces of L . An ordered basis $\mathcal{A} = \{a_1, \dots, a_n\}$ of A is said to be *matched* to ordered basis $\mathcal{B} = \{b_1, \dots, b_n\}$ of B if

$$(1) \quad a_i^{-1}A \cap B \subset \langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle,$$

for each $1 \leq i \leq n$, where $\langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle$ stands for the subspace of B spanned $\{b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n\}$. We say A is *matched* to B (or A is *matchable* to B) if every ordered basis \mathcal{A} of A can be matched to an ordered basis \mathcal{B} of B .

Note that if (1) is the case, then no $a_i b_i$ lie in A and thus $a_i \mapsto b_i$ defined a matching $\mathcal{A} \rightarrow \mathcal{B}$ in the multiplicative group L^* in the group setting. It is established in [17] that $\mathcal{A} = \{a_1, \dots, a_n\}$ is matched to a basis of B if and only

if the following dimension criteria hold for every $J \subset \{1, \dots, n\}$

$$\dim_K \bigcap_{i \in J} (a_i^{-1} A \cap B) \leq n - |J|.$$

In particular, setting $J = \{1, \dots, n\}$, the subspace $\bigcap_{i=1}^n (a_i^{-1} A \cap B)$ must be trivial which cannot occur if $1 \in B$. Having said this, the linear analogue of the matching property is defined as follows.

Definition. A field extension $K \subset L$ is said to have the *linear matching property* if for every finite-dimensional K -subspaces A and B of L with $\dim_K A = \dim_K B$ and $1 \notin B$, A is matched to B .

Similar to the group setting it is proved in [17] that $K \subset L$ possesses the linear matching property if and only if there are no nontrivial finite intermediate extension $K \subset M \subset L$. So the existence of nontrivial finite intermediate extensions is an obstruction for the linear matching property. This observation is formally stated and proven in [2] as follows.

Theorem 4. *Let $K \subset L$ be a field extension and A be an n -dimensional subspace of L which does not contain any linear translate of a nontrivial finite dimensional subfield of L . Then A is matched to any n -dimensional K -subspace of L provided $1 \notin B$.*

Remark 5. Notice that if $K \subset L$ is a field extension, M is an intermediate subfield, and $l \in L^*$, a linear translate of M is a K -subspace of the form lM .

The proof of Theorem 4 is essentially based on the adaptation of methods employed in [17] from the theory of matroids, specifically Rado's Theorem [29], and a linear version of Kneser's theorem (Theorem 8).

In continuation of Theorem 1.4 in [5], where in the linear settings, a sufficient condition for unmatchable subspaces is addressed, we come up with sufficient conditions for the existence of matchable subspaces, similar to Theorem 2 in the group setting. Likewise, certain linear structures of subspaces, such as Sidon subspaces, are leveraged in our results. Note that all necessary definitions are presented in Section 2. In Theorem 6, we assume that $p(K, L)$ denotes the smallest degree of an intermediate field extension $K \subsetneq M \subset L$. Thus $p(K, L) \geq 2$, and $p(K, L) = \infty$ if the extension is purely transcendental. All other necessary definitions concerning Theorem 6 and 7 are provided in Section 2. It is worth mentioning that Theorem 6 parts (1), (2), (3) may be seen as a linear analogue of Theorem 2 parts (1), (4) and (5), respectively.

Theorem 6. *Let $K \subset L$ be a field extension. Let A and B be two n -dimensional K -subspaces in L with $1 \notin B$ and $n > 1$. Assume further that one of the following conditions holds:*

1. $B \cap M = \{0\}$, for every finite dimensional intermediate field $K \subset M \subsetneq L$, and either $n \leq 5$ or every algebraic element of L is separable over K .
2. $n = p(K, L)$ and A is not a linear translate of any nontrivial intermediate field $K \subset M \subsetneq L$.
3. A is a Sidon subspace.

Then A is matched to B .

The following is one of our primary results, wherein unmatchable subspaces are characterized by utilizing the linear structure of subspace B . Note that it may be seen as a linear version of Theorem 3.

Theorem 7. *Let $K \subset L$ be a field extension. Let A be an n -dimensional K -subspace of L . Assume that there exists an n -dimensional K -subspace B with $1 \notin B$ so that A is not matched to B . Then $B \oplus K$ contains a subspace whose 1-atom is a nontrivial intermediate field $K \subsetneq M \subset L$.*

Organization of the paper. Section 2 encompasses all the necessary concepts and results drawn from additive number theory, matching theory, and their linear counterparts. These notions and results serve as the foundation for the proofs presented in our work. Section 3 is dedicated to presenting the proofs of our main results, specifically those related to matchings within the context of abelian groups. Section 4 is focused on providing the proofs related to linear matchings. Finally, in Section 5, we present two conjectures concerning linear matchings. We first explore the possibility of a linear counterpart to a result we have previously proven in the context of matchings within groups (Theorem 2 part (7)). Next, we introduce the concept of Chowla subspaces as a linear analogue of Chowla subsets, and we conjecture whether a similar result to matchings in Chowla subsets can be extended to matchings in Chowla subspaces.

2. PRELIMINARIES

2.1. Abelian additive theory

We commence this section by providing definitions and presenting a few results from additive number theory, along with cardinal criteria for matchable sets. Given an abelian group G and nonempty subsets A, B of G , we define their product as

$$AB = \{ab \mid a \in A, b \in B\}.$$

The subset $A \subset G$ is called a *Sidon subset* if all pairwise products of its elements are distinct. That is, the equation $ab = cd$ has only the trivial solution $\{a, b\} = \{c, d\}$ in A . A nonempty subset A of G , not containing 1, is called a *Chowla subset*

if the order of every element of A is $\geq |A| + 1$. A *progression* of length k , initial term a with common ratio d is a subset of G of the form $\{a, ad, ad^2, \dots, ad^{k-1}\}$. Let H be a nontrivial subgroup of G . The subset $A \subset G$ is called *H-periodic* if it can be expressed as the union of some H -cosets. If A is H -periodic, every element $a \in AH \setminus A$ is called an *H-hole* and thus the number of H -holes in A in view of Proposition 4.1(v) in [19] is

$$|AH| - |A| = |AH \setminus A|.$$

A *quasi-periodic decomposition* of A with *quasi-period* H is a partition $A = A_1 \cup A_0$ of A into two disjoint (two possibly empty) subsets such that A_1 is H -periodic or an H -coset. A set $A \subset G$ is *quasi-periodic* if A has a quasi-periodic decomposition $A = A_1 \cup A_0$ with A_1 nonempty.

The objective of this subsection is to introduce and elucidate one of the most fundamental theorems in Inverse Additive Theory: Kneser's Theorem, along with its numerous variants, extensions, and consequences. There exist several equivalent ways to present Kneser's Theorem. We begin with the following form of this theorem from [27, p.115]. See [19] for further discussion about Kneser's Theorem.

Theorem 8 (Kneser's Theorem). *Let G be an abelian group and A and B be nonempty subsets of G . Then*

$$|AB| \geq |A| + |B| - |H|,$$

where H is the stabilizer of AB , i.e.,

$$H = \{x \in G \mid xAB \subset AB\}.$$

Theorem 8 has the following equivalent formulation whose proof shall be found in [27].

Theorem 9. *Let G, A and B be as in Theorem 8. If $|AB| < |A| + |B| - 1$, then*

$$|AB| \geq |AH| + |BH| - |H|,$$

where $HAB = AB$.

The following result will be used in the proof of Theorem 2 part (7). It is a consequence of Kneser's Theorem together with the *Pigeonhole bounds* for product sets.

Proposition 10. *Let G be an abelian group and A and B be nonempty finite subsets of G . Assume that for every nontrivial finite subgroup H of G and all elements $a, b \in G$, we have*

$$|aH \cap A| + |bH \cap B| \leq |H| + 1.$$

Then for all nonempty subsets $S \subset A$ and $T \subset B$, we have $|ST| \geq |S| + |T| - 1$.

Proof. Assume to the contrary, there exist subsets $S \subset A$, $T \subset B$ such that

$$(2) \quad |ST| < |S| + |T| - 1.$$

Applying Kneser's Theorem to S and T , we have

$$(3) \quad |ST| \geq |SH| + |TH| - |H|,$$

where $HST = ST$.

Combining (2) and (3) together with the fact that $|SH \setminus S| = |SH| - |S|$ and $|TH \setminus T| = |TH| - |T|$ we arrive at the following

$$(4) \quad |SH \setminus S| + |TH \setminus T| \leq |H| - 2.$$

It follows from (4) that there are at most $|H| - 2$ H -holes, namely, elements from $HA \setminus A$ or $HB \setminus B$. Take $a \in S$ and $b \in T$. Since $S \subset A$ and $T \subset B$, so

$$\begin{aligned} |aH \cap A| + |bH \cap B| &\geq |aH \cap S| + |bH \cap T| \\ &\geq 2|H| - (\text{total number of } H\text{-holes}) \\ &\geq 2|H| - (|H| - 2) = |H| + 2, \end{aligned}$$

contradicting our assumptions on A and B . ■

The following theorem [10] is a stronger form of Kneser's addition theorem in the sense that in Kneser's Theorem, the subgroup that stabilizes AB appears to depend on both sets A and B , but in the following theorem, the stabilizer actually may be seen to depend only on A .

Theorem 11. *Let G be an abelian group, and let $A \subset G$ be a finite subset of G . Then*

- *either for every finite subset B of G , we have*

$$|AB| \geq |A| + |B| - 1,$$

- *or there exists a subgroup $H \neq \{e\}$ of G such that, for every finite subset B of G satisfying*

$$|AB| < |A| + |B| - 1,$$

we have $HAB = AB$.

The following result from [13] characterizes relatively large product sets. Essentially, it serves as a generalization of the Cauchy-Davenport Theorem [11, 15] and Chowla's Theorem [12] in the context of abelian groups.

Theorem 12. *Let G be an abelian group and A be a finite subset of G containing the neutral element e . Suppose that for every proper subgroup H of G we have $A \cap H = \{e\}$. Then for any finite subset S of G , we have*

$$|AS| \geq \min\{|G|, |A| + |S| - 1\}.$$

Another result from [13] generalizes Olson's result [28] for the case of abelian groups is a strong building block employed in Theorem 2 parts (2), (3) to ensure matchability in sets that are not contained in a union of certain number of cosets of any proper subgroup of the given abelian group.

Theorem 13. *Let $m \geq 1$ and A_1, \dots, A_m be finite, nonempty subsets of an abelian group G , such that no A_i is contained in a union of l cosets of any proper finite subgroup of G , then*

$$|A_1 \cdots A_m| \geq \min \left\{ |G|, \left(\frac{l}{l+1} + \frac{1}{(l+1)m} \right) \sum_{i=1}^m |A_i| \right\}.$$

The following theorem is well-known as the *Multiplicity Bound* and it arises as a consequence of Kneser's Theorem. This theorem was originally proven by Kemperman [24]. It provides valuable insights into the relationship between the size of the product set AB to the multiplicities of elements within AB .

Theorem 14. *Let G be an abelian group with $A, B \subset G$ finite and nonempty. If $|AB| \leq |A| + |B| - k$, then $r_{A,B}(x) \geq k$, for all $x \in AB$, where*

$$r_{A,B}(x) = |\{(a, b) \in A \times B \mid ab = x\}|.$$

Corollary 15. *Let G be an abelian group and C be a finite Sidon subset of G . If A, B are subsets of G with $AB \subset C$, then $|AB| \geq |A| + |B| - 1$.*

Proof. Since C is a Sidon subset, clearly $r_{A,B}(x) = 1$, for every $x \in AB$. Thus by the contrapositive of Theorem 14, we deduce that $|AB| > |A| + |B| - 2$, implying $|AB| \geq |A| + |B| - 1$. ■

We will take advantage of the following result of Hamidoune [20] to prove Theorem 2, part (6).

Theorem 16. *Let G be an arbitrary group, and let A and B be two proper finite subsets of G such that $A \cup AB \neq A\langle B \rangle$, where $\langle B \rangle$ is the subgroup generated by B . Then $|A \cup AB| \geq |A| + \min\{|B|, v(B)\}$, where $v(B)$ is the minimum order of an element in B .*

The central role in proving Theorem 3 and classifying unmatchable sets based on their additive structures is attributed to the following profound result by Kemperman [25].

Theorem 17. *Let A and B be finite subsets of an abelian group G satisfying $|AB| \leq |A| + |B| - 1$ and $\min\{|A|, |B|\} > 1$. Then either AB is a progression or AB is quasi-periodic.*

While classifying matchable subsets, it is evident that if $AB \cap A = \emptyset$, then A is matched to B . In particular, every bijection from A to B is a matching. Clearly, this represents an extreme situation. On the other end of the spectrum, we encounter a situation where $AB = A$. Then under this condition, A cannot be matched to B . This scenario is explored in [5], and the following proposition is established. This result will be employed in the proof of Theorem 2 part (2).

Proposition 18. *Let A and B be nonempty finite subsets of an arbitrary group G . Assume that $|A| \leq |B|$ and that $AB = A$. Then B is a subgroup of G , and A is a coset of B .*

Similar to the dimension criteria for matchable bases of vector subspaces, cardinality criteria for matchable subsets are discussed and proved in [4] as follows. This result is mainly constructed upon Hall's Marriage Theorem, and Kneser's addition Theorem.

Lemma 19. *Let G be an abelian group and A and B be two finite subsets of G with the same cardinality. Let $A = \{a_1, \dots, a_n\}$. Then A is matched to B if and only if*

$$\left| \bigcap_{i \in J} (a_i^{-1}A \cap B) \right| \leq n - |J|,$$

for all nonempty subset $J \subset \{1, \dots, n\}$.

In addition to works in [26, 16, 2] on classifying matchable sets, Hamidoune in [21] proves the matchability of large classes of sets, in which the concept of Chowla subsets arises.

Theorem 20. *Let A, B be nonempty finite subsets of a group G with $|A| = |B|$. If B is a Chowla subset, then A is matched to B .*

2.2. Linear versions of some addition theorems

Turning our focus to linear adaptations of definitions and results from additive theorems, it is notable that several additive theorems that bound $|AB|$ have been transposed to a linear framework in the following sense. Let $K \subset L$ be a field extension and A, B be K -subspaces of L . We denote by $\langle AB \rangle$ the K -subspace spanned by the product set AB in L . One remarkable development in this line of research is the formulation of a linear counterpart to Kneser's addition theorem,

as presented in [23]. In this section, we will primarily delve into these bounds and their implications on the structures of A and B .

We begin with defining the required notions used in Theorems 6 and 7 starting with the notion of Sidon subspaces. Following [8], we say a K -subspace A of L is a *Sidon subspace* if

$$(5) \quad \forall x \in L \setminus K, \dim_K(A \cap xA) \leq 1.$$

Note that it is discussed in [8] that (5) implies

$$(6) \quad \forall x, y, z, t \in A \setminus \{0\}, xy = zt \Rightarrow \{Kx, Ky\} = \{Kz, Kt\}.$$

In view of (6), the analogy with the Sidon subsets is highlighted.

We continue borrowing some terminologies from [8] to prepare ourselves to define 1-atoms. Let A be a K -subspace of L . For every nonzero finite-dimensional K -subspace X of L , we denote by

$$\partial_A(X) = \dim_K \langle XA \rangle - \dim_K X.$$

Let ψ be the set of nonzero finite-dimensional K -subspaces X of L such that $\langle XA \rangle \neq L$. If ψ is nonempty, we define the *1st-connectivity* of A by

$$\kappa(A) = \min_{X \in \psi} \partial_A(X).$$

If ψ is empty, we set $\kappa(A) \neq -\infty$. We define a *1st-fragment* of A to be an $M \in \psi$ with $\partial_A(M) = \kappa(A)$. A 1st-fragment with minimum dimension is called a *1-atom*.

We now state a linear analogue of Kneser's addition Theorem and its variants and consequences. We begin with the following result from [23] in which the separability condition is imposed on our field.

Theorem 21. *Let $K \subset L$ be a field extension in which every algebraic element of L is separable over K . Let $A, B \subset L$ be nonzero finite dimensional K -subspaces of L and M be the stabilizer of $\langle AB \rangle$, i.e., $M = \{x \in L | x\langle AB \rangle \subset \langle AB \rangle\}$. Then*

$$\dim_K \langle AB \rangle \geq \dim_K A + \dim_K B - \dim_K M.$$

Remark 22. It is proved in [22] that the separability condition in Theorem 21 can be removed in the price of imposing the assumption $\dim_K A \leq 5$.

The separability condition in Theorem 21 is removed in the following Theorem from [9] in the sense that two scenarios turn out for the dimension of $\langle AB \rangle$, depending on the stabilizer of one of the subspaces. That is, in contrast to Theorem 21 the subfield M seems to depend on both A and B , in Theorem 23 the stabilizer basically may be seen to depend on only one of the subspaces.

Theorem 23. *Let $K \subset L$ be a field extension and $A \subset L$ be a K -subspace of L of finite positive dimension. Then*

- *either for every finite-dimensional subspace B of L , we have*

$$\dim_K \langle AB \rangle \geq \dim_K A + \dim_K B - 1,$$

- *or there exists an intermediate field $K \subset M \subset L$, such that for every finite-dimensional subspace B of L satisfying*

$$\dim_K \langle AB \rangle < \dim_K A + \dim_K B - 1,$$

we have $\langle AB \rangle M = \langle AB \rangle$.

The following theorem from [8] is not as powerful as the linear analogue of Kneser's Theorem but it is useful in classifying unmatchable subspaces with respect to the structural features of subspaces addressed in Theorem 7.

Theorem 24. *Let $K \subset L$ be a field extension. Let S be a K -subspace of L containing 1. Let A be the 1-atom of S . If there exists a K -subspace T of L for which*

$$\dim_K \langle ST \rangle < \dim_K S + \dim_K T - 1 < \dim_K L,$$

then A is a subfield of L properly containing K .

As discussed earlier in Section 1, we addressed a dimension criterion proposed by Eliahou-Lecouvey [17] to characterize matchable bases. This criterion serves as a fundamental cornerstone in our proofs for theorems relating to matchable and unmatchable subspaces. In light of its significance in our work, we present it here for reference.

Theorem 25. *Let $K \subset L$ be a field extension and A, B be n -dimensional K -subspaces of L . Let $\mathcal{A} = \{a_1, \dots, a_n\}$ be a basis of A . Then \mathcal{A} can be matched to a basis of B if and only if for all nonempty $J \subset \{1, \dots, n\}$, we have*

$$\dim_K \bigcap_{i \in J} (a_i^{-1} A \cap B) \leq n - |J|.$$

2.3. Linear matchings in primitive subspaces

Primitive subspaces are initially introduced in [3] as a linear counterpart to a set of generating elements in a given cyclic group. Given a separable field extension $K \subset L$, a K -subspace A of L is called a *primitive subspace* if $K(a) = L$ for every $a \in A \setminus \{0\}$. Primitive subspaces have been studied in two aspects. First, such subspaces seem interesting in their own right. For example, in [1, 4] the size of the largest primitive subspace in a separable field extension is investigated and

determined. Second, when dealing with a primitive subspace B , it is proved in [3] that every subspace A with $\dim_K A = \dim_K B$ is matched to B . Theorem 6 part (1) generalizes this result. Moreover, in Section 5, we define Chowla subspaces that are a wider class of vector spaces and speculate on the notion of matchability when replacing primitive subspaces with Chowla subspaces.

3. PROOFS ON MATCHING IN ABELIAN GROUPS

Proof of Theorem 2. For any subset S of A , let $V_S := \{b \in B \mid Sb \subset A\}$ and $W_S := V_S \cup \{e\}$. We will first prove that each of conditions (1) through (7) implies $|SW_S| \geq |S| + |W_S| - 1$.

Part (1). Since $B \cap H = \emptyset$, for every proper subgroup H of G , we conclude that $W_S \cap H = \{e\}$. Applying Theorem 12 to S and W_S we have

$$(7) \quad |SW_S| \geq \min\{|G|, |S| + |W_S| - 1\}.$$

On the other hand,

$$|SW_S| \leq |A| = |B| < |G|,$$

since $SW_S \subset A$ and $B \subsetneq G$.

This along with (7) implies that $|SW_S| \geq |S| + |W_S| - 1$.

Part (2). Applying Theorem 13 to S and W_S , we have

$$(8) \quad |SW_S| \geq \min \left\{ |G|, \left(\frac{l}{l+1} + \frac{1}{2(l+1)} \right) (|S| + |W_S|) \right\}.$$

In a similar manner as in part (1), we may argue that $|SW_S| < |G|$. Thus

$$(9) \quad |SW_S| \geq \left(\frac{l}{l+1} + \frac{1}{2(l+1)} \right) (|S| + |W_S|).$$

Clearly $|S| + |W_S| \leq 2n + 1$. We claim that $|S| + |W_S| \neq 2n + 1$, as otherwise, $|S| = n$ and $|V_S| = n$, implying $S = A$ and $V_S = B$. Thus $B? = \{b \in B \mid Ab \subset A\}$ entailing $AB = B$. It follows from Proposition 18 that B is a subgroup of G , contradicting $e \notin B$. So $|S| + |W_S| \leq 2n$. We have

$$2l + 2 \geq 2n \geq |S| + |W_S|.$$

Therefore,

$$1 \geq \frac{1}{2l+2} (|S| + |W_S|) = \left(1 - \frac{l}{l+1} - \frac{1}{2(l+1)} \right) (|S| + |W_S|).$$

Hence,

$$(10) \quad \left(1 - \frac{l}{l+1} - \frac{1}{2(l+1)}\right) (|S| + |W_S|) \geq |S| + |W_S| - 1.$$

Combining (9) and (10), we have $|SW_S| \geq |S| + |W_S| - 1$, as claimed.

Part (3). Applying Theorem 13 to S and W_S , along with the argument used in part (2), we obtain that

$$(11) \quad |SW_S| \geq \left(1 - \frac{l}{l+1} - \frac{1}{2(l+1)}\right) (|S| + |W_S|).$$

We claim that $|S| + |W_S| \leq 2n - 1$. Clearly, $|S| + |W_S| \leq 2n + 1$. Additionally, in a similar manner as in part (2), we may argue that $|S| + |W_S| \neq 2n + 1$. So it is left to show $|S| + |W_S| \neq 2n$. Assume to the contrary, $|S| + |W_S| = 2n$. This means $|S| + |V_S| = 2n - 1$. We split into two cases.

Case 1. $|S| = n$ and $|V_S| = n - 1$. So $S = A$ and $V_S = V_A$ with $|V_A| = n - 1$. Let $B = \{b_1, \dots, b_n\}$ and without loss of generality, assume $V_S = \{b_1, \dots, b_{n-1}\}$. Thus, $Ab_i \subset A$, for every $1 \leq i \leq n - 1$. Since $|Ab_i| = |A|$, we conclude that $Ab_i = A$, for $1 \leq i \leq n - 1$. Therefore,

$$\prod_{a \in A} a = \prod_{a \in A} ab_1 = \prod_{a \in A} ab_2 = \dots = \prod_{a \in A} ab_{n-1}.$$

Thus, $a^n = a^n b_i^n$ entailing $b_i^n = e$, $1 \leq i \leq n - 1$. This contradicts B having at least two elements with orders greater than n .

Case 2. $|S| = n - 1$ and $|V_S| = n$. Let $A = \{a_1, \dots, a_n\}$. Without loss of generality, assume that $S = \{a_1, \dots, a_{n-1}\}$. Clearly $V_S = B$. Thus, $SB \subset A$. So $a_i B \subset A$, for all $1 \leq i \leq n - 1$. Since $|a_i B| = |B| = |A|$, hence $a_i B = A$, for all $1 \leq i \leq n - 1$. Therefore,

$$\prod_{j=1}^n a_j = \prod_{j=1}^n a_1 b_j = \prod_{j=1}^n a_2 b_j = \dots = \prod_{j=1}^n a_{n-1} b_j,$$

entailing $a_i^n = a_j^n$, for all $1 \leq i, j \leq n - 1$. This contradicts $|\{a^n | a \in A\}| > 2$.

So in both cases, we extract contradictions, and then $|S| + |W_S| < 2n - 1$. We have

$$2l + 2 \geq 2n - 2 \geq |S| + |W_S|,$$

implying

$$1 \geq \frac{1}{2l+2} (|S| + |W_S|).$$

In a similar manner as in part (2), one may conclude that

$$(12) \quad \left(\frac{l}{l+1} + \frac{1}{2(l+1)} \right) (|S| + |W_S|) \geq |S| + |W_S| - 1.$$

Combining (11) and (12), we obtain $|SW_S| \geq |S| + |W_S| - 1$, as claimed.

Part (4). Applying Theorem 11 to S and W_S , we either have $|SW_S| \geq |S| + |W_S| - 1$ or $|SW_S| < |S| + |W_S| - 1$, and there exist a subgroup $H \neq \{e\}$ of G with $SW_S H = SW_S$. Suppose that the latter case satisfies. Then we have

$$(13) \quad |H| \leq |SW_S H| = |SW_S| \leq |A| = p(G).$$

It follows from (13) that $|H| = p(G)$. Therefore $|SW_S H| = |A|$. On the other hand $SW_S H = SW_S \subset A$. Thus $SW_S H = A$. Choose $x \in SW_S$, then $xH \subset A$ and since $|xH| = |H| = p(G) = |A|$, then $xH = A$, contradicting A not being a coset of any nontrivial subgroup of G . Therefore $|SW_S| \geq |S| + |W_S| - 1$, as claimed.

Part (5). Since $SW_S \subset A$ and A is a Sidon subset, applying Corollary 15 to S and W_S one may have $|SW_S| \geq |S| + |W_S| - 1$.

Part (6). We are going to apply Theorem 16 to S and V_S .

We show that $S \cup SV_S \neq S\langle V_S \rangle$; otherwise since $SV_S \cup S \subset A$, we would conclude that $S\langle V_S \rangle \subset A$. Therefore, if $a \in S$ and $b \in V_S$, $a\langle b \rangle \subset A$. Since $o(b) \geq n$, then $|a\langle b \rangle| \geq |A|$, implying $A = a\langle b \rangle$ and $o(b) = n$. Thus $A = \{a, ab, \dots, ab^{n-1}\}$, contradicting A not being a progression. Now applying Theorem 16 to S and V_S , we have

$$\begin{aligned} |SW_S| &= |S(V_S \cup \{e\})| = |SV_S \cup S| \\ &\geq |S| + \min\{|V_S|, o(b); b \in V_S\} = |S| + |V_S| \\ &= |S| + |W_S| - 1, \end{aligned}$$

as desired.

Part (7). Let $B_0 = B \cup \{e\}$. Then we have

$$|aH \cap A| + |bH \cap B_0| \leq |H| + 1,$$

for every nontrivial finite subgroup H of G and $a, b \in G$. Applying Proposition 10 to A and B_0 , we conclude that $|SW_S| \geq |S| + |W_S| - 1$, as $S \subset A$ and $W_S \subset B_0$.

Therefore in all parts (1)-(7), we established that $|SW_S| \geq |S| + |W_S| - 1$, which implies that $|V_S| \leq n - |S|$. On the other hand, $V_S = \bigcap_{a_i \in S} (a_i^{-1} A \cap B)$, for every $S \subset A$. Therefore $|\bigcap_{a_i \in S} (a_i^{-1} A \cap B)| \leq n - |S|$. Invoking Lemma 19, we conclude that A is matched B . \blacksquare

Corollary 26. *Let $A, B \subset \mathbb{Z}_n$ where $|A| = |B|$ and $\gcd(b, n) = 1$, for every $b \in B$. Then A is matched to B .*

Proof. Since $\gcd(b, n) = 1$ for every $b \in B$, it follows that $B \cap H = \emptyset$, for every proper subgroup H of \mathbb{Z}_n (indeed the condition $\gcd(b, n) = 1$ implies that every $b \in B$ is a generating element of \mathbb{Z}_n . So if $a \in B \cap H = \emptyset$, we may conclude that $\mathbb{Z}_n = \langle b \rangle \subset H \subset G$, contradicting H being a proper subgroup of \mathbb{Z}_n .) Invoking Theorem 2 part (1), we conclude that A is matched to B . ■

Remark 27. Theorem 2 part (1) is a strengthening of a result from [26], establishing that all abelian torsion-free groups and cyclic groups of prime orders possess the matching property.

Remark 28. Theorem 2 part (2) is a strengthening of Theorem 1. Furthermore, a theorem by Losonczy [24] asserts that all abelian torsion-free groups and all cyclic groups of prime order possess the matching property. This can be regarded as a consequence of Theorem 2 part (2).

Remark 29. Theorem 2, part (6) represents a modest strengthening of Theorem 20 wherein the condition $\text{ord}(x) \geq |B| + 1$, for every $x \in B$ is replaced with $\text{ord}(x) \geq |B|$, in the price of imposing the extra assumption of A not being a progression.

Example 30. Consider the subsets $A = \{5, 6, 7\}$ and $B = \{1, 2, 3\}$ of \mathbb{Z}_{15} . \mathbb{Z}_{15} has two nontrivial proper subgroups: $H = \{0, 5, 10\}$ and $K = \{0, 3, 6, 9, 12\}$. Upon examination, it becomes evident that neither A nor B can be written as a 2-union of cosets of H (and K). By Theorem 2 part (2), A is matched to B .

Example 31. Consider the subsets $A = \{1, 2, 3, 9, 14\}$ and $B = \{4, 5, 6, 10, 13\}$. It can be verified that both A and B satisfy the conditions of Theorem 2, part (3), with $l = 3$ and $n = 5$. Consequently, A is matched to B .

Example 32. Let A be a maximal Sidon subset of \mathbb{Z}_{2^m} . Invoking Proposition 2.8 in [14], if $m = 7$, then $|A| = 12$. This is attained if $A = \{0, 1, 2, 4, 8, 16, 32, 64, 15, 60, 101, 87\}$. It follows from Theorem 2, part (5) that A is matched to every subset of \mathbb{Z}_{128} with $|B| = 12$ and $0 \notin B$.

Example 33. Consider $A = \{1, 8, 15, 22, 30\} \subset \mathbb{Z}_{35}$. Clearly $|A| = 5 = p(\mathbb{Z}_{35})$ and A is not a coset of the subgroup $K = \{0, 7, 14, 21, 28\}$ of \mathbb{Z}_{35} . Following Theorem 2 part (4), A is matched to every subset B of \mathbb{Z}_{35} with $|B| = 5$ and $0 \notin B$.

Example 34. Consider the subsets $A = \{0, 4, 8\}$ and $B = \{3, 6, 8\}$ of \mathbb{Z}_9 . Then for every $a, b \in \mathbb{Z}_9$, $|(a + H) \cap A| + |(b + H) \cap B| < 4$, where $H = \{0, 3, 6\}$ is the only proper subgroup of \mathbb{Z}_9 . It follows from Theorem 2 part (7) that A is matched to B .

3.1. Matchings and coset representatives in abelian groups

Let G be a finite abelian group and H a subgroup of G . If g_1, \dots, g_m are elements such that the cosets H_{g_1}, \dots, H_{g_m} are distinct and cover the entirety of G , we call these elements *coset representatives*. Every nonempty subset of a coset representative is called a *semicoset representative*. Let A and B be two subsets of \mathbb{Z}_{p^2} , where p is prime, $|A| = |B| = n \leq p$ and $0 \notin B$. Suppose both A and B are coset representatives or semicoset representatives. Then A and B are not contained in the union of $n - 1$ cosets of H , where H is the subgroup of \mathbb{Z}_{p^2} with $|H| = p$. By Theorem 2 part (2), A must be matched to B .

Proof of Theorem 3. Let $A = \{a_1, \dots, a_n\}$. Since A is not matched to B , by Lemma 19, there must exist $J \subset \{1, \dots, n\}$ such that

$$(14) \quad \left| \bigcap_{i \in J} (a_i^{-1}A \cap B) \right| > n - |J|.$$

Set $S = \{a_i | i \in J\}$, $V = \bigcap_{i \in J} (a_i^{-1}A \cap B)$ and $W = V \cup \{e\}$. Then by (14), one can derive $|V| + |S| > n$. Therefore,

$$(15) \quad |W| + |S| - 1 > n.$$

On the other hand, since $SW \subset A$, it follows from (15) that

$$(16) \quad |SW| < |W| + |S| - 1.$$

We claim that $\min\{|S|, |W|\} > 1$. If this were not the case, we would have either $|S| = 1$ or $|W| = 1$. If $|S| = 1$, it would imply that $S = \{a\}$, for some $a \in A$. Thus,

$$|SW| = |aW| = |W| = |W| + |S| - 1.$$

This would lead to a contradiction with (16).

Similarly, if $|W| = 1$, it would mean $W = \{e\}$ and we would again have a contradiction, as

$$|SW| = |Se| = |S| = |S| + |W| - 1.$$

So $\min\{|S|, |W|\} > 1$. Applying Theorem 17 to S and W , we may conclude that either SW forms a progression or SW is quasi-periodic. Since $SW \subset A$, then the first case implies a progression subset for A and the second case yields a quasi-periodic subset for A . Both of these cases contradict our initial assumptions on A . ■

4. PROOFS ON MATCHING SUBSPACES IN A FIELD EXTENSION

Proof of Theorem 6. Let $\mathcal{A} = \{a_1, \dots, a_n\}$ be any bases of A . For every nonempty $J \subset \{1, \dots, n\}$, denote $S = \langle a_i | i \in J \rangle$, the subspace spanned by $\{a_i | i \in J\}$ and

$$V_S = \bigcap_{i \in J} (a_i^{-1} A \cap B) = \{x \in B \mid a_i x \in A \text{ for all } i \in J\}.$$

Clearly $\dim_K S = |J|$. Define $W_S = K \oplus V_S$ yielding $\dim_K W_S = \dim_K V_S + 1$ and $SW_S \subset A$. We claim that the following inequality holds true in each part of our theorem

$$\dim_K \langle SW_S \rangle \geq \dim_K S + \dim_K W_S - 1,$$

and we validate each part independently.

Part (1). Let us begin by assuming that every algebraic element of L is separable over K . Applying Theorem 21 to S and W_S , there must exist an intermediate field $K \subset M \subset L$ such that

$$(17) \quad \dim_K \langle SW_S \rangle \geq \dim_K S + \dim_K W_S - \dim_K M,$$

where $M \langle SW_S \rangle = \langle SW_S \rangle$.

Let us introduce $W'_S = \langle M \cup V_S \rangle$. Using Theorem 21 once again, we acquire the inequality

$$(18) \quad \dim_K \langle SW'_S \rangle \geq \dim_K S + \dim_K W'_S - \dim_K M',$$

where M' is the stabilizer of $\langle SW_S \rangle$.

Now, it becomes evident that $\langle SW'_S \rangle = \langle SW_S \rangle$ because

$$\begin{aligned} \langle SW'_S \rangle &= \langle S(M \cup V_S) \rangle \\ &= \langle S(M \cup W_S) \rangle \\ &= \langle SM \cup SW_S M' \rangle \\ &= M \langle S \cup SW_S \rangle \\ &= M \langle SW_S \rangle \\ &= \langle SW_S \rangle. \end{aligned}$$

Given that $\langle SW'_S \rangle = \langle SW_S \rangle$, it is clear that they share the same stabilizer, implying that $M = M'$. This, together with (18), we obtain

$$\dim_K \langle SW'_S \rangle \geq \dim_K S + \dim_K W'_S - \dim_K M,$$

entailing

$$(19) \quad \begin{aligned} \dim_K \langle SW_S \rangle &\geq \dim_K S + \dim_K W_S - \dim_K M \\ &= \dim_K S + \dim_K \langle M \cup V_S \rangle - \dim_K M. \end{aligned}$$

Now, utilizing (19) together with the inclusion-exclusion principle for vector spaces, we derive

$$(20) \quad \begin{aligned} \dim_K \langle SW_S \rangle &\geq \dim_K S + \dim_K M + \dim_K V_S - \dim_K (M \cap V_S) - \dim_K M \\ &= \dim_K S + \dim_K V_S - \dim_K (M \cap V_S). \end{aligned}$$

Since $M \cap B = \{0\}$ and $V_S \subset B$, it follows that $M \cap V_S = \{0\}$. This along with (20), we conclude that

$$\dim_K \langle SW_S \rangle \geq \dim_K S + \dim_K V_S = \dim_K S + \dim_K W_S - 1,$$

as claimed.

A similar line of reasoning may be employed to prove that

$$\dim_K \langle SW_S \rangle \geq \dim_K S + \dim_K W_S - 1,$$

in case $n \leq 5$, applicable to general field extensions, in light of Remark 22.

Part (2). Assume, for the sake of contradiction, that

$$\dim_K \langle SW_S \rangle < \dim_K S + \dim_K W_S - 1.$$

Then by Theorem 23, there exists an intermediate field $K \subsetneq M \subset L$ with $M \langle SW_S \rangle = \langle SW_S \rangle$. Given that $\langle SW_S \rangle \subset A$, we may deduce

$$(21) \quad \dim_K M \leq \dim_K M \langle SW_S \rangle = \dim_K \langle SW_S \rangle \leq \dim_K A = p(K, L).$$

Since $\dim_K M \leq p(K, L)$ and $K \subsetneq M$, it follows that $\dim_K M = p(K, L) = n$. Choose a nonzero element $x \in \langle SW_S \rangle$. Then $Mx \subset M \langle SW_S \rangle = \langle SW_S \rangle \subset A$. On the other hand, $\dim_K Mx = \dim_K M = n = \dim_K A$. Consequently, we arrive at the contradictory result that $Mx = A$, which contradicts the assumption that A is not a linear translate of any nontrivial intermediate field within $K \subset M \subsetneq L$.

Part (3). Suppose, for the sake of contradiction, that

$$(22) \quad \dim_K \langle SW_S \rangle < \dim_K S + \dim_K W_S - 1.$$

By applying Theorem 23, we can deduce the existence of an intermediate field $K \subsetneq M \subset L$ such that $M \langle SW_S \rangle = \langle SW_S \rangle$. Choose a nonzero element $x \in M \setminus K$. Then $x \langle SW_S \rangle \subset \langle SW_S \rangle$. Moreover, considering the dimension, we observe that

$\dim_K x\langle SW_S \rangle = \dim_K \langle SW_S \rangle$. Hence $x\langle SW_S \rangle = \langle SW_S \rangle$. Since A is a Sidon subspace, we have $\dim_K(xA \cap A) \leq 1$. Given that $\langle SW_S \rangle \subset A$, we conclude that

$$\begin{aligned} 1 &\geq \dim_K(xA \cap A) \geq \dim_K \langle x\langle SW_S \rangle \cap \langle SW_S \rangle \rangle \\ &= \dim_K \langle SW_S \rangle = \dim_K \langle S \cup SV_S \rangle \geq \dim_K S. \end{aligned}$$

As a result, we find that $\dim_K S = 1$ as $S \neq \{0\}$. Now, it follows from (22) that $\dim_K \langle SW_S \rangle < \dim_K W_S$, which is impossible.

In all parts (1)–(3), we have demonstrated that

$$\dim_K \langle SW_S \rangle \geq \dim_K S + \dim_K W_S - 1,$$

which implies that $\dim_K V_S \leq n - |J|$, for every $J \subset \{1, \dots, n\}$. Therefore, according to Theorem 25, we conclude that A is matched to B . ■

Remark 35. Theorem 4.2 from [3] is a direct consequence of Theorem 3, part (1). In other words, if B is a primitive subspace in a separable field extension $K \subset L$, then it is evident that $B \cap M = \{0\}$, for every intermediate field $K \subset M \subsetneq L$. Therefore, the assumption of Theorem 2, part (1) holds, and A is matched to B .

Remark 36. Suppose $K \subset L$ is a field extension that is purely transcendental or $[L : K] = p$, for some prime p . In both cases, every algebraic element of L is separable over K . That is, in purely transcendental situation, $L \setminus K$ has no algebraic element over K , and in the prime degree of extension, the extension is simple and thus separable. Therefore, it follows from Theorem 6 part (1) that $K \subset L$ possesses the linear matching property.

Example 37. Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[35]{2})$. Let B be the \mathbb{Q} -subspace of $\mathbb{Q}(\sqrt[35]{2})$ spanned by $\sqrt[35]{2}$, $\sqrt[35]{4}$ and $\sqrt[35]{8}$. Then, firstly, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[35]{2})$ is separable, and secondly, $B \cap M = \{0\}$, for every intermediate field $\mathbb{Q} \subsetneq M \subset \mathbb{Q}(\sqrt[35]{2})$. Then by Theorem 6, part (1), every 3-dimensional \mathbb{Q} -subspace A of $\mathbb{Q}(\sqrt[35]{2})$ is matched to B .

Proof of Theorem 7. Given that A is not matched to B , we can invoke Theorem 25, which leads to the existence of a basis $\mathcal{A} = \{a_1, \dots, a_n\}$ for A and a subset $J \subset \{1, \dots, n\}$ such that

$$\dim_K \bigcap_{i \in J} (a_i^{-1} A \cap B) > n - |J|.$$

Set $V_J := \bigcap_{i \in J} (a_i^{-1} A \cap B)$, $W_J := K \oplus V_J$ and $S_J = \langle a_i \mid i \in J \rangle$. Then we have

$$\dim_K \langle S_J W_J \rangle < \dim_K S_J + \dim_K W_J - 1.$$

Now, let M denote the 1-atom of W_J . We can deduce from Theorem 24 that M is a subfield of L properly containing K . That is, $B \oplus K$ contains a subspace W_J whose 1-atom M is a subfield of L properly containing K , as asserted. ■

5. TWO CONJECTURES

5.1. Linear analogue of Theorem 2, part (7)

In Theorem 2 part (7), we basically deal with matchability between sets A and B whose all nonempty subsets $S \subset A$ and $T \subset B$ satisfy the condition $|ST| \geq |S| + |T| - 1$. It is evident that this result relies on Proposition 10. It is tempting to speculate that Proposition 10 can be extended to a linear setting. If such an extension is successfully established, it could be employed to provide a linear analogue for Theorem 2 part (7) in some obvious manners. Having said this, we formulate the following conjecture.

Conjecture 38. *Let $K \subset L$ be a field extension and $A, B \subset L$ be a K -subspace of L of finite positive dimensions. Assume further that for every $a, b \in L$ and every nontrivial proper finite intermediate subfield $K \subset M \subsetneq L$, we have*

$$\dim_K(aM \cap A) + \dim_K(bM \cap B) \leq [M : K] + 1.$$

Then for all K -subspaces $S \subset A$ and $T \subset B$, the following holds

$$\dim_K \langle ST \rangle \geq \dim_K S + \dim_K T - 1.$$

5.2. Matchings in Chowla subspaces

In light of Hamidoune's findings [21] regarding matchable sets A and B , with B being a Chowla subset, we aim to formulate a linear analogue of Chowla subsets and explore potential linear matchings in this setting. Consider a field extension $K \subset L$ and let A be a K -subspace of L . We define A as a Chowla subspace if, for every $a \in A \setminus \{0\}$, we satisfy the condition $[K(a) : K] \geq \dim_K A + 1$. Notably, within a finite separable field extension, every primitive subspace is a Chowla subspace. Therefore, it follows, based on Theorem 2.7 in [1], that the maximum attainable dimension of a Chowla K -subspace in L is greater than or equal to

$$[L : K] - \max_{K \subset M \subsetneq L} [M : K],$$

where M is a proper intermediate field.

Now, a natural question to ponder is: In separable (or general) field extensions, what is the upper bound on the size of a Chowla subspace? Additionally, it would be quite valuable if one could investigate the following question, serving as a linear counterpart to Theorem 20, which asserts that in the abelian group context, if $|A| = |B|$ with B being a Chowla subset, then A must be matched to B .

Conjecture 39. *Let $K \subset L$ be a field extension and A and B be two n -dimensional K -subspaces of L . If B is a Chowla subspace, then A is matched to B .*

Acknowledgement

We are thankful to David Gryniewicz for discussions on Kneser's addition theorem and its implications, which have been truly valuable.

REFERENCES

- [1] M. Aliabadi and K. Filom, *Results and questions on matchings in abelian groups and vector subspaces of fields*, J. Algebra **598** (2022) 85–104.
<https://doi.org/10.1016/j.jalgebra.2022.01.025>
- [2] M. Aliabadi, M. Hadian and A. Jafari, *On matching property for groups and field extensions*, J. Algebra Appl. **15**(1) (2016) 1650011.
<https://doi.org/10.1142/S0219498816500110>
- [3] M. Aliabadi and M.V. Janardhanan, *On local matching property in groups and vector space*, Australas. J. Combin. **70** (2018) 75–85.
- [4] M. Aliabadi and M. V. Janardhanan, *On matchable subsets in abelian groups and their linear analogues*, Linear Algebra Appl. **582** (2019) 138–155.
<https://doi.org/10.1016/j.laa.2019.08.007>
- [5] M. Aliabadi, J. Kinseth, C. Kunz, H. Serdarevic and C. Willis, *Conditions for matchability in groups and field extensions*, Linear and Multilinear Algebra **71**(7) (2023) 1182–1197.
<https://doi.org/10.1080/03081087.2022.2057903>
- [6] M. Aliabadi and S. Zerbib, *Matchings in matroids over abelian groups* (arXiv preprint arXiv:2202.07719).
arXiv:2022
<https://doi.org/10.1007/s10801-024-01308-z>
- [7] N. Alon, C.K. Fan, D. Kleitman and J. Losonczy, *Acyclic matchings*, Adv. Math. **122**(23) (1996) 234–236.
<https://doi.org/10.1006/aima.1996.0060>
- [8] C. Bachoc, O. Serra and G. Zémor, *An analogue of Vosper's theorem for extension fields*, Mathematical Proceedings of the Cambridge Philosophical Society **163** (2017) 423–452.
<https://doi.org/10.1017/S0305004117000044>
- [9] C. Bachoc, O. Serra and G. Zémor, *Revisiting Kaeser's theorem for field extensions*, Combinatorica **38**(4) (2018) 759–777.
<https://doi.org/10.1007/s00493-016-3529-0>
- [10] É. Balandraud, *Une variante de la méthode isopérimétrique de Hamidoune, appliquée au théorème de Kneser*, Annales de l'institut Fourier **58**(3) (2008) 915–943.
<https://doi.org/10.5802/aif.2374>
- [11] A. Cauchy, *Recherches sur les nombres*, J. Ecole Polytechnique **9** (1813) 99–116.

- [12] I. Chowla, *A theorem on the addition of residue classes: Application to the number $\gamma(k)$ in Waring's problem*, Proceedings of the Indian Academy of Sciences-Section A **2(3)** (1935) 242–243.
- [13] T. Cochrane, M. Ostergaard and C. Spencer, *Cauchy-davenport theorem for abelian groups and diagonal congruences*, Proceedings of the American Mathematical Society **147(8)** (2019) 3339–3345.
<https://doi.org/10.1090/proc/14468>
- [14] I. Czerwinski and A. Pott, *Sidon sets, sum-free sets and linear codes* (<https://arxiv.org/abs/2304.07906>).
arXiv:2023
<https://arxiv.org/abs/2304.07906>
- [15] H. Davenport, *On the addition of residue classes*, J. Lond. Math. Soc. **1(1)** (1935) 30–32.
<https://doi.org/10.1112/jlms/s1-10.37.30>
- [16] S. Eliahou and C. Lecouvey, *Matchings in arbitrary groups*, Adv. Appl. Math. **40(2)** (2008) 219–224.
<https://doi.org/10.1016/j.aam.2006.12.001>
- [17] S. Eliahou and C. Lecouvey, *Matching subspaces in a field extensio*, J. Algebra **324(12)** (2010) 3420–3430.
<https://doi.org/10.1016/j.jalgebra.2010.09.026>
- [18] C. K. Fan and J. Losonczy, *Matchings and canonical forms for symmetric tensors*, Adv. Math. **117(2)** (1996) 228–238.
<https://doi.org/10.1006/aima.1996.0010>
- [19] D.J. Grynkiewicz, *Structural additive theory* (30, Springer).2013
- [20] Y.O. Hamidoune, *A generalization of an addition theorem of Shatrowsky*, Eur. J. Combin. **13(4)** (1992) 249–255.
[https://doi.org/10.1016/S0195-6698\(05\)80031-9](https://doi.org/10.1016/S0195-6698(05)80031-9)
- [21] Y.O. Hamidoune, *Counting certain pairings in arbitrary groups*, Combin., Probab. Comput. **20(6)** (2011) 855–865.
<https://doi.org/10.1017/S0963548311000459>
- [22] X.D. Hou, *On a vector space analogue of Kneser's theorem*, Linear Algebra Appl. **426(1)** (2007) 214–227.
<https://doi.org/10.1016/j.laa.2007.04.019>
- [23] X.D. Hou, K. Leung and Q. Xiang, *A generalization of an addition theorem of Kneser*, J. Number Theory **97(1)** (2002) 1–9.
<https://doi.org/10.1006/jnth.2002.2793>
- [24] J.H.B. Kemperman, *On small sumsets in an abelian group*, Acta Math. **103** (1960) 63–88.
<https://doi.org/10.1007/BF02546525>

- [25] J.H.B. Kemperman, *On complexes in a semigroup*, in: Indagationes Mathematicae, 59 (Ed(s)) (Elsevier, 1956) 247–254.
[https://doi.org/10.1016/S1385-7258\(56\)50032-7](https://doi.org/10.1016/S1385-7258(56)50032-7)
- [26] J. Losonczy, *On matchings in groups*, Adv. Appl. Math. **20(3)** (1998) 385–391.
<https://doi.org/10.1006/aama.1998.0587>
- [27] M. Nathanson, Additive number theory: Inverse problems and the geometry of sumsets (Springer-Verlag, New York, 1996).
- [28] J. Olson, *On the sum of two sets in a group*, J. Number Theory **18(1)** (1984) 110–120.
- [29] R. Rado, *A theorem on independence relations*, Quarterly J. Math. **1(1)** (1942) 83–89.
<https://doi.org/10.1093/qmath/os-13.1.83>
- [30] E.K. Wakeford, *On canonical forms*, Proceedings of the London Mathematical Society **2(1)** (1920) 403–410.
<https://doi.org/10.1112/plms/s2-18.1.403>

Received 13 November 2023

Revised 6 April 2024

Accepted 7 April 2024