

CHARACTERIZATION OF MATCHABLE SETS AND SUBSPACES VIA DYSON TRANSFORMS

MOHSEN ALIABADI¹ AND JOZSEF LOSONCZY^{2,*}

ABSTRACT. A *matching* from a finite subset A of an abelian group G to another subset B is a bijection $f : A \rightarrow B$ such that $af(a) \notin A$ for all $a \in A$. The study of matchings began in the 1990s and was motivated by a conjecture of E. K. Wakeford on canonical forms for homogeneous polynomials. The theory was later extended to the linear-algebraic setting of vector subspaces over field extensions, and then to matroids. In this paper, we investigate the existence and structure of matchings in both abelian groups and field extensions. Using Dyson's e -transform, a tool from additive combinatorics, along with a linear analogue which is introduced in this paper, we establish characterization theorems for matchable sets and subspaces. Several applications are given to demonstrate the effectiveness of these theorems as standalone tools. Throughout, we highlight the parallels between the group-theoretic and linear-algebraic perspectives.

1 Introduction

History of matchings. A geometric framework for a class of bipartite graphs was introduced in [?], where a special type of perfect matching, termed an acyclic matching, was defined and shown to exist for certain graphs using geometric techniques. The existence of such matchings is closely tied to the non-vanishing of determinants of specific weighted biadjacency matrices. This setup was applied to a conjecture of E. K. Wakeford [?] which dates to 1916 and involves determining the sets of monomials that can be eliminated from a generic homogeneous polynomial through linear changes of variables.

In a notable special case, Wakeford's conjecture was reduced to the problem of showing that acyclic matchings exist for certain pairs of subsets in \mathbb{Z}^n . The full conjecture remains open, but the acyclic matching property introduced in [?] was later shown to hold in the most general sense for \mathbb{Z}^n by Alon et al. [?], and was completely characterized for all abelian groups in [?]. Further developments appeared in [?], where a broader class of matchings was investigated in abelian groups. The theory was then

¹Department of Mathematics, University of California, San Diego, 9500 Gilman Dr, La Jolla, CA 92093, USA. maliabadisr@ucsd.edu.

²Department of Mathematics, Long Island University, 720 Northern Blvd, Brookville, New York 11548, USA. Jozsef.Losonczy@liu.edu.

*Corresponding Author.

Keywords and phrases. Chowla set, Chowla subspace, linear matching property, matchable sets, Sidon set.

2020 Mathematics Subject Classification. Primary: 05D15; Secondary: 11B75; 12F99.

extended to arbitrary groups by Eliahou and Lecouvey [?]. Related counting aspects were explored by Hamidoune [?].

A linear formulation of matchings was introduced in [?], providing an analogue in the setting of field extensions, while a matroidal version was proposed in [?]. A recent application of matchings in abelian groups within combinatorial number theory can be found in [?].

Organization of paper. In the following two sections, we first revisit a pair of foundational results on matchings which will be used in the abelian group setting (Section ??), and then transition to the linear-algebraic framework, outlining the necessary background information on matchable subspaces over field extensions (Section ??). Building upon these backgrounds, Sections ?? and ?? present our main contributions, offering characterizations of matchable sets in abelian groups and matchable subspaces in field extensions, respectively, as stated in Theorems ?? and ?. We will also give several applications to show that these theorems are effective tools on a standalone basis, eliminating a longstanding reliance on a variety of inequalities from additive number theory and related areas.

1.1. Preliminaries on matchings (abelian group setting)

Let A and B be nonempty finite sets of the same cardinality, and let \mathcal{G} be a subset of $A \times B$. A bijective mapping $f : A \rightarrow B$ is called a *matching* of \mathcal{G} if $(a, f(a)) \in \mathcal{G}$ for all $a \in A$. Note that A and B are not required to be disjoint.

For $S \subseteq A$ and $T \subseteq B$, we define

$$\mathcal{G}_1(S) = \{b \in B : (a, b) \in \mathcal{G} \text{ for some } a \in S\},$$

$$\mathcal{G}_2(T) = \{a \in A : (a, b) \in \mathcal{G} \text{ for some } b \in T\},$$

and for $a \in A$ and $b \in B$, let $d_1(a) = |\mathcal{G}_1(\{a\})|$ and $d_2(b) = |\mathcal{G}_2(\{b\})|$. In the first part of the paper, where we consider matchings in abelian groups, we will make use of two well-known results from matching theory. For convenience, we state them here using the above notation. Proofs can be found in [?]. The first is Philip Hall's marriage theorem, which gives a necessary and sufficient condition for the existence of a matching.

Theorem 1.1 (P. Hall). *Let A and B be nonempty finite sets such that $|A| = |B|$, and let \mathcal{G} be a subset of $A \times B$. Then there exists a matching of \mathcal{G} if and only if for every nonempty subset S of A , we have $|S| \leq |\mathcal{G}_1(S)|$.*

The other result, attributed to Marshall Hall, is useful for establishing a lower bound on the number of matchings.

Theorem 1.2 (M. Hall). *Let A and B be nonempty finite sets such that $|A| = |B|$, let \mathcal{G} be a subset of $A \times B$, and let n be a positive integer. Assume that there exists at least one matching of \mathcal{G} , and that for each $b \in B$, we have $d_2(b) \geq n$. Then there are at least $n!$ matchings of \mathcal{G} .*

We are interested in a certain group-theoretic context for the sets A , B , and \mathcal{G} . Let G be an abelian group (with operation written multiplicatively) and let A and B be nonempty finite subsets of G such that $|A| = |B|$. Define \mathcal{G} by

$$\mathcal{G} = \{(a, b) \in A \times B : ab \notin A\}.$$

In this paper, we will always assume that \mathcal{G} is as above. A matching of \mathcal{G} is then a bijection $f : A \rightarrow B$ satisfying $af(a) \notin A$ for all $a \in A$. We will usually not mention \mathcal{G} explicitly and instead refer to such an f as a “matching from A to B .”

Example 1.3. Let G be a cyclic group of order 6, and let x be a generator. Take $A = \{1, x^2, x^4, x^5\}$ and $B = \{x, x^2, x^3, x^4\}$. Then there is no matching from A to B , since, for the subset $S = \{1, x^2, x^4\}$ of A , we have $\mathcal{G}_1(S) = \{x, x^3\}$, so that the condition in Theorem ?? is violated. If instead we take B to be the set $\{x, x^2, x^3, x^5\}$, then there are exactly two matchings from A to B ; one is given by $1 \mapsto x, x^2 \mapsto x^5, x^4 \mapsto x^3, x^5 \mapsto x^2$, and the other is the mapping $1 \mapsto x^3, x^2 \mapsto x, x^4 \mapsto x^5, x^5 \mapsto x^2$.

The number of matchings (possibly 0, as we just saw above) turns out to be related to the arithmetic structures of A and B , as well as the algebraic structure of G .

It will be convenient to have a version of Theorem ?? which is tailored to our group-theoretic setup. Given a subset S of A , let

$$U = \{b \in B : Sb \subseteq A\}.$$

Then $B \setminus U = \mathcal{G}_1(S)$. Therefore, we have the following:

Corollary 1.4. *Let G be an abelian group, and let A and B be nonempty finite subsets of G such that $|A| = |B|$. Then there exists a matching from A to B if and only if for every nonempty subset S of A , we have $|S| \leq |B \setminus U|$, where $U = \{b \in B : Sb \subseteq A\}$.*

We conclude with the simple observation that a necessary condition for the existence of a matching from A to B is $1 \notin B$. For A and B contained in certain abelian groups G , this condition is also sufficient (see Corollary ?? for a precise statement).

1.2. Preliminaries on matchings (linear setting)

For any positive integer n , we use $[n]$ to denote the set $\{1, \dots, n\}$. Given a subset S of a vector space V , we write $\langle S \rangle$ for the subspace of V spanned by S . If $S = \{x_1, \dots, x_n\}$, we may also denote this subspace by $\langle x_1, \dots, x_n \rangle$.

The notion of matching two subspaces in a field extension, as described below, was introduced by Eliahou and Lecouvey in [?].

Let $K \subseteq L$ be a field extension, and let A and B be two n -dimensional K -subspaces of L , with $n > 0$. An ordered basis $\mathcal{A} = \{a_1, \dots, a_n\}$ of A is said to be *matched* to an ordered basis $\mathcal{B} = \{b_1, \dots, b_n\}$ of B if

$$a_i^{-1}A \cap B \subseteq \langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle \quad \text{for each } i \in [n].$$

We say that A is *matched* to B (or is *matchable* to B) if every ordered basis of A can be matched to some ordered basis of B .

Note that if the above condition holds, then $a_i b_i \notin \mathcal{A}$ for all i , so the map $a_i \mapsto b_i$ defines a matching, in the group-theoretic sense, from \mathcal{A} to \mathcal{B} in the multiplicative group L^\times .

Remark 1.5. A necessary condition for A to be matched to B is that $1 \notin B$. This is discussed in detail in [?]; however, to keep the presentation here as self-contained as possible, we repeat their argument.

Assume that A is matched to B , and suppose, for the sake of contradiction, that $1 \in B$. Let $\mathcal{A} = \{a_1, \dots, a_n\}$ be a basis of A . Then \mathcal{A} is matched with a basis $\mathcal{B} = \{b_1, \dots, b_n\}$. By definition, we have

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

for each $i \in [n]$. This implies

$$1 \in \bigcap_{i \in [n]} (a_i^{-1} A \cap B) \subseteq \bigcap_{i \in [n]} \langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle = \{0\},$$

which is a contradiction.

A field extension $K \subseteq L$ is said to have the *linear matching property* if for every pair of finite-dimensional K -subspaces A and B of L with $\dim A = \dim B > 0$ and $1 \notin B$, the subspace A is matched to B .

In the second part of the paper, where we examine matchings in the linear setting, we make use of an analogue of P. Hall's marriage theorem (Theorem ??), expressed in the language of systems of distinct representatives.

Let V be a finite-dimensional vector space over a field K , and let $\mathcal{W} = \{W_i\}_{i \in [n]}$ be a family of subspaces of V . A *free transversal* for \mathcal{W} is a linearly independent set of vectors $\{x_1, \dots, x_n\} \subseteq V$ such that $x_i \in W_i$ for each $i \in [n]$.

A fundamental result of Rado [?] provides a necessary and sufficient condition for the existence of a free transversal, closely resembling the condition in P. Hall's classical marriage theorem.

Theorem 1.6 (Rado). *Let V be a finite-dimensional vector space over a field K , and let $\mathcal{W} = \{W_i\}_{i \in [n]}$ be a family of subspaces of V . Then \mathcal{W} admits a free transversal if and only if*

$$\dim \left(\sum_{i \in J} W_i \right) \geq |J| \quad \text{for all } J \subseteq [n].$$

Given a field extension $K \subseteq L$ and K -subspaces A and B of L , we use AB to denote the *Minkowski product* of A and B :

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

By combining Rado's theorem with linear analogues of two theorems from additive number theory, Eliahou and Lecouvey [?] established the following fundamental results:

- A subspace A is matched to itself if and only if $1 \notin A$.

- A field extension $K \subseteq L$ has the linear matching property if and only if L contains no nontrivial proper finite-dimensional extension over K .

The main objective of our work in the linear setting is to develop an efficient and unified framework for characterizing pairs of matchable subspaces, one that not only recovers known results but also provides a definitive perspective on the underlying structure of the pairs.

2 Matchings in abelian groups

Let G be an abelian group and let S be a subset of G . In this section, the notation $\langle S \rangle$ is used for the subgroup of G generated by S . If $S = \{x\}$, then we also write $\langle x \rangle$ for this subgroup. We use $o(x)$ for the order of any $x \in G$, with the understanding that $o(x) = \infty$ if x does not have finite order.

The following is the first main result of this paper. Its proof will rely on Dyson's e -transform, which is discussed in Chapter 2 of [?]. Note, however, that our particular use of the e -transform will not require any background knowledge concerning its properties.

Theorem 2.1. *Let A and B be nonempty finite subsets of an abelian group G such that $|A| = |B|$ and $1 \notin B$. Then there exists a matching from A to B if and only if for every pair of nonempty subsets $S \subseteq A$ and $R \subseteq B \cup \{1\}$ such that $SR = S$, we have $|S| \leq |B \setminus R|$.*

Proof. Assume that there is a matching from A to B . Suppose S and R are nonempty sets satisfying $S \subseteq A$, $R \subseteq B \cup \{1\}$, and $SR = S$. We will show that $|S| \leq |B \setminus R|$.

Let $U = \{b \in B : Sb \subseteq A\}$. Since there is a matching from A to B , it follows from Corollary ?? that

$$|S| \leq |B \setminus U|.$$

Observe that R is a subset of $U \cup \{1\}$, since $R \subseteq B \cup \{1\}$ and $SR = S \subseteq A$. Hence

$$B \setminus (U \cup \{1\}) \subseteq B \setminus R.$$

We have $1 \notin B$, so this inclusion can be simplified to $B \setminus U \subseteq B \setminus R$, which implies

$$|B \setminus U| \leq |B \setminus R|.$$

Combining our inequalities gives $|S| \leq |B \setminus R|$, as desired.

Assume, conversely, that the condition in the statement involving S and R holds. We will show that there is a matching from A to B by verifying that the condition in Corollary ?? is satisfied.

Let S be a nonempty subset of A . As above, define $U = \{b \in B : Sb \subseteq A\}$. We will show that $|S| \leq |B \setminus U|$. Let $R = U \cup \{1\}$. We consider two cases.

Case 1: $SR = S$. We can apply our hypothesis to S and R , to obtain

$$|S| \leq |B \setminus R|.$$

Since $1 \notin B$, we have $B \setminus R = B \setminus U$, and so

$$|S| \leq |B \setminus U|,$$

as desired.

Case 2: $SR \neq S$. We will employ Dyson's e -transform. Let $e \in S$ and $r \in R$ be such that $er \notin S$. Define sets S_1 and R_1 by

$$\begin{aligned} S_1 &= S \cup (eR), \\ R_1 &= R \cap (Se^{-1}). \end{aligned}$$

We claim that the following conditions hold:

- (i) $S_1 R_1 \subseteq SR \subseteq A$,
- (ii) $|S_1| + |R_1| = |S| + |R|$,
- (iii) $1 \in R_1 \subseteq R \subseteq B \cup \{1\}$,
- (iv) $S_1 \subseteq A$ and $|S| < |S_1|$.

Conditions (i) and (iii) follow directly from the definitions of S , R , S_1 , and R_1 . Regarding (iv), we have $S_1 \subseteq A$ on account of (i) and (iii) (specifically, $S_1 R_1 \subseteq A$ and $1 \in R_1$). The rest of (iv) follows from the fact that $S \subseteq S_1$ and $er \in S_1 \setminus S$. Finally, to see that (ii) holds, observe that

$$\begin{aligned} |S_1| &= |S \cup (eR)| \\ &= |S| + |eR| - |S \cap (eR)| \\ &= |S| + |R| - |S \cap (eR)|, \end{aligned}$$

and the map

$$\begin{aligned} R_1 &\longrightarrow S \cap (eR) \\ x &\mapsto xe \end{aligned}$$

is a bijection.

If $S_1 R_1 \neq S_1$, we repeat the above, replacing S with S_1 and R with R_1 . The process continues until we reach nonempty sets S_m and R_m satisfying $S_m R_m = S_m$. This must eventually occur because the sets S_1, S_2, \dots are strictly increasing in size and are contained in the finite set A . Note that the sets S_m and R_m must satisfy

- (v) $S_m R_m = S_m \subseteq A$,
- (vi) $|S_m| + |R_m| = |S| + |R|$,
- (vii) $1 \in R_m \subseteq R \subseteq B \cup \{1\}$.

Applying our hypothesis to S_m, R_m (note that (v) and (vii) ensure that S_m, R_m can play the roles of S, R), we get

$$|S_m| \leq |B \setminus R_m|.$$

Since $1 \notin B$, we can rewrite this inequality as

$$|S_m| \leq |B \setminus (R_m \setminus \{1\})|.$$

We have $1 \in R_m$ and $R_m \setminus \{1\} \subseteq R \setminus \{1\} = U \subseteq B$, hence

$$\begin{aligned} |S_m| &\leq |B| - |R_m \setminus \{1\}| \\ &= |B| - |R_m| + 1. \end{aligned}$$

Finally, using (vi) and bearing in mind that $|R| - 1 = |U|$, we obtain

$$|S| \leq |B| - |U| = |B \setminus U|,$$

so that the condition in Corollary ?? holds. \square

The lemma below recalls a known interpretation of the condition $SR = S$ in Theorem ?? in terms of cosets. It will be used frequently in the applications.

Lemma 2.2. *Let G be an abelian group and let S and R be nonempty finite subsets of G . Then $SR = S$ if and only if S is a union of cosets of $\langle R \rangle$.*

Proof. Assume that $SR = S$. Let $a \in S$. For any $x \in R$, we have $ax \in SR = S$ and by induction $ax^k \in S$ for all positive integers k . Since S is finite, it follows that $o(x) < \infty$. Thus $\langle x \rangle = \{x, x^2, \dots, x^{o(x)}\}$ and clearly $a\langle x \rangle \subseteq S$. Note, in particular, that $ax^{-1} = ax^{o(x)-1} \in S$.

Now suppose $x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$ is a word on R , with each ϵ_i equaling ± 1 , and $a' \in S$. By the above paragraph, $a'x_1^{\epsilon_1} \in S$, hence $(a'x_1^{\epsilon_1})x_2^{\epsilon_2} \in S$, and so on, giving us $a'x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \in S$. Thus $a'\langle R \rangle \subseteq S$. From this we see that S is a union of cosets of $\langle R \rangle$.

The converse is clear. \square

Let G be an abelian group. A subset of G of the form $\{a, ax, \dots, ax^{n-1}\}$, where $a, x \in G$ and n is a positive integer such that $n - 1 < o(x)$, is called a *progression of length n* .

The following result is new and can be viewed as a generalization of Theorem 1.2-(6) in [?].

Corollary 2.3. *Let A and B be nonempty finite subsets of an abelian group G such that $|A| = |B|$ and $1 \notin B$. Let n be a positive integer. Assume that A contains no progression of length greater than n , and every element of B has order greater than n . Then there exists a matching from A to B .*

Proof. Suppose S and R are nonempty sets such that $S \subseteq A$, $R \subseteq B \cup \{1\}$, and $SR = S$. We claim that $R = \{1\}$. Let $x \in R$ and $a \in S$. Then $a\langle R \rangle \subseteq S$ by Lemma ?? . Also, we must have $o(x) \leq n$; otherwise, the set $\{ax, ax^2, \dots, ax^{n+1}\}$ would be a progression of length greater than n contained in $a\langle R \rangle \subseteq S \subseteq A$. On the other hand, every element of B is assumed to have order greater than n , so x cannot belong to B . Since $R \subseteq B \cup \{1\}$, we then must have $x = 1$. The claim is established.

It follows that $|B \setminus R| = |B \setminus \{1\}| = |B| = |A| \geq |S|$. We now apply Theorem ?? to complete the proof. \square

A *Chowla subset* of a (not necessarily abelian) group G is a nonempty subset S with the property that every element of S has order greater than $|S|$. In [?], Hamidoune used the isoperimetric method to prove that if A and B satisfy the usual conditions and, in addition, B is a Chowla subset of G , then there is a matching from A to B . In the case where G is abelian, this result follows easily from our work above.

Corollary 2.4. *Let A and B be nonempty finite subsets of an abelian group G such that $|A| = |B|$ and $1 \notin B$. If B is a Chowla subset of G , then there exists a matching from A to B .*

Proof. Take $n = |A| = |B|$ in Corollary ??.

□

Remark 2.5. We mention that Corollary ?? can be used to derive Corollary 3.6 in [?]. Let A and B be nonempty finite subsets of an abelian group G such that $1 \notin B$ and $|A| = |B| = n < n(G)$, where $n(G)$ denotes the smallest cardinality of a nontrivial subgroup of G . In this situation, B is a Chowla subset, and thus, by Corollary ??, there is a matching from A to B .

Next, we provide a short proof, using Theorem ??, of a result which first appeared in [?]. We point out that, in the argument below, the verification of the condition in Theorem ?? involving S and R is rather different from the one given for Corollary ??.

Corollary 2.6. *Let A be a nonempty finite subset of an abelian group G such that $1 \notin A$. Then there exists a matching from A to itself.*

Proof. Suppose S and R are nonempty sets such that $S \subseteq A$, $R \subseteq A \cup \{1\}$, and $SR = S$. Then S and R are disjoint. To see this, assume the contrary and let $a \in S \cap R$. Then $\langle R \rangle = a\langle R \rangle$ and, by Lemma ??, $a\langle R \rangle \subseteq S$. Hence $1 \in S \subseteq A$, a contradiction.

By the above and the fact that $S \cup (R \setminus \{1\}) \subseteq A$, we have $|S| + |R \setminus \{1\}| \leq |A|$, and so

$$|S| \leq |A| - |R \setminus \{1\}| = |A \setminus (R \setminus \{1\})| = |A \setminus R|.$$

Applying Theorem ?? completes the proof.

□

Let A be a finite subset of an abelian group G . We say that A is a *Sidon set* if every x in G can be written in at most one way as a product $x = a_1 a_2$, with $a_1, a_2 \in A$, up to a transposition of the factors. It was shown in [?] (see Theorem 1.2-(5)) that if $A \subseteq G$ is a nonempty Sidon set, then for any subset B of G of the same size as A with $1 \notin B$, there is a matching from A to B . Below, we establish a lower bound for the number of such matchings.

Corollary 2.7. *Let A and B be nonempty finite subsets of an abelian group G such that $|A| = |B|$ and $1 \notin B$. Assume that A is a Sidon set. Then there are at least $(|A| - 1)!$ matchings from A to B .*

Proof. To estimate the number of matchings, we will apply Theorem ??. By Theorem 1.2-(5) in [?], we know that there is at least one matching, but we will prove this fact here in a different way in order to give another example of the applicability of Theorem ??. Suppose S and R are nonempty sets such that $S \subseteq A$, $R \subseteq B \cup \{1\}$, and $SR = S$. We will show that $R = \{1\}$. Let $x \in R$ and $a \in S$. By Lemma ??, $a\langle R \rangle$ is a subset of S , and hence of A .

Observe that $o(x) \leq 2$, since otherwise a, ax, ax^2 would be distinct elements of $a\langle R \rangle$ satisfying $(ax)(ax) = (ax^2)a$, contradicting the Sidon property of A . In fact, we cannot have $o(x) = 2$ because this would mean that the elements $a \neq ax$ satisfy $aa = (ax)(ax)$, another contradiction. Thus $R = \{1\}$. By Theorem ??, there is a matching from A to B .

To use Theorem ??, we also need to show that $d_2(b) \geq |A| - 1$ for each $b \in B$. Assume the contrary. Then there exist $b \in B$ and distinct $a_1, a_2 \in A$ such that $a_1 b, a_2 b \in A$.

Let $y_1 = a_1b$ and $y_2 = a_2b$. Then $b = a_1^{-1}y_1 = a_2^{-1}y_2$, hence $a_2y_1 = a_1y_2$ (note that $a_1 \neq y_1$, since b cannot equal 1). This contradiction to the Sidon assumption completes the proof. \square

An abelian group G is said to have the *matching property* if for all pairs of nonempty finite subsets A and B of G with $|A| = |B|$ and $1 \notin B$, there exists a matching from A to B . The result below, which first appeared in [?], characterizes the groups G having the matching property. The original proof relied on a theorem of Kneser; the one that follows uses Theorem ??.

Corollary 2.8. *Let G be an abelian group. Then G has the matching property if and only if G is torsion-free or of prime order.*

Proof. First observe that the trivial group has the matching property and is torsion-free, so we may assume $|G| > 1$ in what follows.

Suppose G is torsion-free or of prime order, and let A and B be nonempty finite subsets of G such that $|A| = |B|$ and $1 \notin B$. We will use Theorem ?? to show that there is a matching from A to B .

As usual, let S and R be nonempty sets such that $S \subseteq A$, $R \subseteq B \cup \{1\}$, and $SR = S$. Let $a \in S$ and note that $a\langle R \rangle \subseteq S$ by Lemma ??. Hence

$$|\langle R \rangle| = |a\langle R \rangle| \leq |S| \leq |A|,$$

from which we see that $\langle R \rangle$ is finite and unequal to G . By hypothesis, G has no nontrivial proper finite subgroups, whence $\langle R \rangle = \{1\}$. We can now apply Theorem ??.

Conversely, assume that G is neither torsion-free nor of prime order. Then G has a nontrivial proper finite subgroup H . Choose $g \in G \setminus H$ and define $A = H$ and $B = (H \setminus \{1\}) \cup \{g\}$. Then $2 \leq |A| = |B| < \infty$, $1 \notin B$, and there is no matching from A to B , since every $b \in B \setminus \{g\}$ satisfies $Hb = H$. \square

For our final application of Theorem ??, we present a generalization of a result on the existence of matchings which appeared recently in [?] (see Theorem 1.2-(7)).

Corollary 2.9. *Let A and B be nonempty finite subsets of an abelian group G such that $|A| = |B|$ and $1 \notin B$. Assume that for every $a \in G$ and every nontrivial proper finite subgroup H of G , we have*

$$|aH \cap A| + |H \cap B| < |H| + 1.$$

Then there exists a matching from A to B .

Proof. Suppose S and R are nonempty sets satisfying $S \subseteq A$, $R \subseteq B \cup \{1\}$, and $SR = S$. Let $a \in S$ and observe, as before, that $a\langle R \rangle \subseteq S$ by Lemma ??. Hence $\langle R \rangle$ is finite and proper. Assume for a contradiction that $\langle R \rangle$ is nontrivial, and note that this implies $\langle R \rangle \cap B \neq \emptyset$. Applying our hypothesis (taking $H = \langle R \rangle$), we get

$$|a\langle R \rangle \cap A| + |\langle R \rangle \cap B| < |\langle R \rangle| + 1.$$

Since $a\langle R \rangle \subseteq A$, this simplifies to

$$|\langle R \rangle| + |\langle R \rangle \cap B| < |\langle R \rangle| + 1,$$

forcing $\langle R \rangle \cap B = \emptyset$, a contradiction. We thus have $R = \{1\}$, enabling us to apply Theorem ??.

□

3 Matching subspaces in a field extension

We first adopt the following conventional notation. For a K -vector space V , the dual space of V is denoted by V^* . Thus,

$$V^* = \{f : V \rightarrow K \mid f \text{ is a } K\text{-linear mapping}\}.$$

For any subspace $W \subseteq V$, we define its annihilator W^\perp in V^* by

$$W^\perp = \{f \in V^* \mid W \subseteq \ker f\}.$$

It is a standard result that if V is finite dimensional,

$$\dim W^\perp = \dim V - \dim W.$$

The following is our second main result. It is the linear counterpart to Theorem ??. We note that the approach taken here parallels that in the abelian group setting, where Dyson's e -transform plays a central role. In the proof below, we introduce and employ a linear analogue of the e -transform, which, to the best of our knowledge, has not been previously investigated and may be of independent interest.

Theorem 3.1. *Let $K \subsetneq L$ be a field extension, and let A and B be two n -dimensional K -subspaces of L , with $n > 0$ and $1 \notin B$. Then A is matched to B if and only if for every pair of nonzero K -subspaces $S \subseteq A$ and $R \subseteq B \oplus K$ with $\langle SR \rangle = S$, we have*

$$\dim S \leq \dim(B/(R \cap B)).$$

Proof. Assume that A is matched to B . Suppose S and R are nonzero subspaces satisfying $S \subseteq A$ and $R \subseteq B \oplus K$ with $\langle SR \rangle = S$. Let $\mathcal{S} = \{a_1, \dots, a_\ell\}$ be a basis for S . We will show that $\dim(R \cap B) \leq n - \ell$. Extend \mathcal{S} to a basis $\mathcal{A} = \{a_1, \dots, a_\ell, a_{\ell+1}, \dots, a_n\}$ for A . Since A is matched to B , there exists a basis $\mathcal{B} = \{b_1, \dots, b_n\}$ for B such that \mathcal{A} is matched to \mathcal{B} . Thus,

$$a_i^{-1}A \cap B \subseteq \langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle \quad \text{for each } i \in [n].$$

This implies

$$(1) \quad \bigcap_{i \in [\ell]} (a_i^{-1}A \cap B) \subseteq \bigcap_{i \in [\ell]} \langle \mathcal{B} \setminus \{b_i\} \rangle = \langle b_{\ell+1}, \dots, b_n \rangle.$$

On the other hand, since $\langle SR \rangle = S$, one has $a_i R \subseteq S$ for each $i \in [\ell]$, and hence $R \subseteq a_i^{-1}S \subseteq a_i^{-1}A$. Therefore,

$$R \cap B \subseteq \bigcap_{i \in [\ell]} (a_i^{-1}A \cap B).$$

Combining this with (1), we have $\dim(R \cap B) \leq n - \ell$, which implies

$$\dim S \leq \dim(B/(R \cap B)),$$

as desired.

Conversely, assume that the condition in the statement involving S and R holds. We will show that A is matched to B . Let $\mathcal{A} = \{a_1, \dots, a_n\}$ be a basis for A . Let $J \subseteq [n]$ be nonempty. Define $S = \langle a_i : i \in J \rangle$, $T = \bigcap_{i \in J} (a_i^{-1}A \cap B)$ and $R = T \oplus K$. We claim that $\dim T \leq n - |J|$. Our argument splits into two cases.

Case 1: $\langle SR \rangle = S$. By our hypothesis, we have

$$\dim S \leq \dim(B/(R \cap B)).$$

Since $T \subseteq B$, $R = T \oplus K$ and $1 \notin B$, it follows that $T = R \cap B$, and so

$$\dim T = \dim(R \cap B) \leq n - |J|,$$

as claimed.

Case 2: $\langle SR \rangle \neq S$. Then $S \subsetneq SR$. Choose $e \in S$ and $r \in R$ such that $er \in SR \setminus S$. Define subspaces S_1 and R_1 as follows:

$$\begin{aligned} S_1 &= S + eR, \\ R_1 &= R \cap (Se^{-1}). \end{aligned}$$

We claim that the following conditions hold:

- (i) $\langle S_1 R_1 \rangle \subseteq \langle SR \rangle \subseteq A$.
- (ii) $\dim S_1 + \dim R_1 = \dim S + \dim R$.
- (iii) $1 \in R_1 \subseteq R \subseteq B \oplus K$.
- (iv) $S_1 \subseteq A$ and $\dim S < \dim S_1$.

Condition (iii) and the first inclusion in (i) follow directly from the definitions of S , R , S_1 , and R_1 .

To verify (ii), we first apply the dimension of a sum formula for vector subspaces:

$$\begin{aligned} \dim S_1 &= \dim(S + eR) \\ &= \dim S + \dim eR - \dim(S \cap eR) \\ &= \dim S + \dim R - \dim(S \cap eR). \end{aligned}$$

Now observe that the map $x \mapsto xe$ defines a linear isomorphism from $R \cap (Se^{-1})$ to $S \cap (eR)$, since $e \neq 0$. This implies

$$\dim R_1 = \dim(R \cap (Se^{-1})) = \dim(S \cap eR),$$

so

$$\dim S_1 + \dim R_1 = \dim S + \dim R,$$

confirming (ii).

Concerning (iv) and the second inclusion in (i), we proceed as follows. By construction, we have

$$ST \subseteq A.$$

Since $R = T \oplus K$, it follows that

$$SR = S(T \oplus K) \subseteq \langle ST \cup S \rangle \subseteq A,$$

and hence $\langle SR \rangle \subseteq A$. In particular,

$$eR \subseteq SR \subseteq A.$$

Also, we have $S \subseteq A$ by the definition of S . Therefore,

$$S_1 = S + eR \subseteq A.$$

Moreover, S_1 properly contains S , since $er \in S_1 \setminus S$. Hence

$$\dim S < \dim S_1.$$

All four conditions have been verified. Now if $\langle S_1 R_1 \rangle \neq S_1$, we repeat the above procedure, substituting S_1 for S and R_1 for R . This iterative process continues until we obtain nonzero subspaces S_m and R_m such that $\langle S_m R_m \rangle = S_m$. Termination is guaranteed, as A is finite-dimensional and the sequence of subspaces S_1, S_2, \dots strictly increases in dimension.

At the final step, the subspaces S_m and R_m satisfy:

- (v) $\langle S_m R_m \rangle = S_m \subseteq A$,
- (vi) $\dim S_m + \dim R_m = \dim S + \dim R$,
- (vii) $1 \in R_m \subseteq R \subseteq B \oplus K$.

By applying our hypothesis to S_m and R_m , which is justified by (v) and (vii), we obtain

$$\dim S_m \leq \dim(B/(R_m \cap B)).$$

Since $\dim(R_m \cap B) = \dim R_m - 1$, it follows that

$$\dim S_m + \dim R_m \leq n + 1,$$

which, combined with (vi) and the fact that $\dim R = \dim T + 1$, yields

$$\dim T \leq n - |J|,$$

as claimed.

So in both cases we have $\dim T \leq n - |J|$. Passing to the annihilator in the dual space B^* , we obtain

$$\dim T^\perp \geq |J|,$$

which leads to

$$\dim \left(\sum_{i \in J} (a_i^{-1} A \cap B)^\perp \right) \geq |J|.$$

Applying Theorem ?? to the family $\{(a_i^{-1} A \cap B)^\perp\}_{i \in [n]}$, we obtain a free transversal $\{f_1, \dots, f_n\} \subseteq B^*$ such that

$$(2) \quad f_i \in (a_i^{-1} A \cap B)^\perp \quad \text{for each } i \in [n].$$

Note that $\{f_1, \dots, f_n\}$ is a basis for B^* .

Let $\mathcal{B} = \{b_1, \dots, b_n\}$ be the basis of B dual to $\{f_1, \dots, f_n\}$. We show that \mathcal{A} is matched to \mathcal{B} . Observe, $f_i(b_j) = \delta_{ij}$, and so

$$\ker f_i = \langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle \quad \text{for each } i \in [n].$$

This combined with (??) gives us

$$a_i^{-1}A \cap B \subseteq \langle b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n \rangle \quad \text{for each } i \in [n],$$

as desired. Therefore, A is matched to B , completing the proof. \square

We will need some basic notation from field theory. If $K \subseteq L$ is a field extension and $x \in L$, we write $K(x)$ for the subfield of L generated by $K \cup \{x\}$, and $[K(x) : K]$ for the dimension of $K(x)$ as a vector space over K . If x is algebraic over K , we write $m_x(t)$ for its minimal polynomial; recall that $\deg m_x(t) = [K(x) : K]$.

The following lemma provides insight into how the condition $\langle SR \rangle = S$ from Theorem ?? will be used in applications.

Lemma 3.2. *Let $K \subseteq L$ be a field extension, let n be a positive integer, let S and R be nonzero K -subspaces of L , and let $x \in R$. Assume that $\langle SR \rangle = S$ and $\dim S \leq n$. Then x is algebraic over K and in fact $[K(x) : K] \leq n$. Also, for each $a \in S$, we have $aK(x) \subseteq S$.*

Proof. Suppose $a \in S$. Note that both conclusions hold when $x = 0$, and the second conclusion holds when $a = 0$. Assume $x, a \neq 0$.

We have $ax \in \langle SR \rangle = S$ and by induction $ax^k \in S$ for all positive integers k . Since $\dim S \leq n$, there exist scalars $c_1, \dots, c_{n+1} \in K$, not all 0, such that

$$\sum_{i=1}^{n+1} c_i ax^i = 0.$$

Multiplying through by $(ax)^{-1}$ gives us

$$\sum_{i=1}^{n+1} c_i x^{i-1} = 0,$$

which shows that x is algebraic over K and moreover that the minimal polynomial $m_x(t)$ has degree at most n . Thus $[K(x) : K] \leq n$.

For the last part of the lemma, note that $x^k \in a^{-1}S$ for all $k \geq 1$, and also $1 \in a^{-1}S$ because $a \in S$. Since every element of $K(x)$ can be written in the form $p(x)$ for some polynomial $p(t)$ in $K[t]$, it follows that $K(x)$ is contained in the K -subspace $a^{-1}S$, and hence $aK(x) \subseteq S$. \square

Let $K \subseteq L$ be a field extension, and let A be a K -subspace of L . We say that A is a *Chowla subspace* if for every $a \in A \setminus \{0\}$, we have

$$[K(a) : K] \geq \dim A + 1.$$

Note that if A is a Chowla subspace, then $1 \notin A$.

The above definition first appeared in [?] and was motivated by Hamidoune's findings [?] concerning matchable subsets A and B of a group, where B is a Chowla subset. Also in [?], a potential for matchings in the linear setting, with B a Chowla subspace,

was conjectured (Conjecture 5.2). The result below provides an affirmative answer to this conjecture.

Corollary 3.3. *Let $K \subsetneq L$ be a field extension, and let A and B be two n -dimensional K -subspaces of L , with $n > 0$. Assume that B is a Chowla subspace. Then A is matched to B .*

Proof. We will use Theorem ?? . Suppose $S \subseteq A$ and $R \subseteq B \oplus K$ are nonzero subspaces such that $\langle SR \rangle = S$.

We claim that $R = K$. To see this, assume the contrary. Choose a nonzero element $a \in S$ and an element $x \in R \setminus K$. Note that, since S is contained in A , we have $\dim S \leq n$. By Lemma ?? ,

$$[K(x) : K] = \deg m_x(t) \leq n.$$

On the other hand, since x lies in $R \subseteq B \oplus K$ but not in K , we can write $x = b + c$, where $b \in B \setminus \{0\}$ and $c \in K$. Note that b must be algebraic over K , since x and c are, and moreover $m_b(t)$ has the same degree as $m_x(t)$ since $m_b(t) = m_x(t + c)$. We now use the fact that B is a Chowla subspace to obtain

$$[K(x) : K] = [K(b) : K] \geq n + 1,$$

a contradiction. The claim is proved.

Since $1 \notin B$, the claim gives us $R \cap B = \{0\}$. Therefore, $\dim S \leq n = \dim(B/(R \cap B))$. We apply Theorem ?? to complete the proof. \square

Remark 3.4. Note that Corollary ?? can be used to derive the commutative case of Theorem 5.5 from [?], which addresses the matchability of small subspaces.¹

Let $K \subsetneq L$ be a field extension, and let $A, B \subseteq L$ be n -dimensional K -subspaces with $1 \notin B$. Suppose $n < n_0(K, L)$, where $n_0(K, L)$ denotes the smallest degree of an intermediate field extension $K \subsetneq F \subseteq L$. Under this assumption, B is a Chowla subspace of L , and by Corollary ?? , the subspace A is matched to B .

Next, we use Theorem ?? to recover, in the commutative setting, Theorem 2.8 in [?]. This result is a linear analogue of Corollary ?? .

Corollary 3.5. *Let $K \subsetneq L$ be a field extension, and let A be a nonzero finite-dimensional K -subspace of L . Then A is matched to itself if and only if $1 \notin A$.*

Proof. Assume that $1 \notin A$. Suppose $S \subseteq A$ and $R \subseteq A \oplus K$ are nonzero K -subspaces such that $\langle SR \rangle = S$. To apply Theorem ?? , we need to show that

$$\dim S \leq \dim(A/(R \cap A)).$$

We claim that $S \cap R = \{0\}$. Assume the contrary and let x be a nonzero element of $S \cap R$. Note that S is finite dimensional, since it is contained in A . By Lemma ?? , x is

¹We note that the results in [?] cited in this paper are stated and proved in the more general setting of a skew field extension $K \subseteq L$, where K is contained in the center of L .

algebraic over K . We write out its minimal polynomial as follows:

$$m_x(t) = c_0 + c_1t + \dots + c_{n-1}t^{n-1} + t^n,$$

where $n > 0$ and $c_0, \dots, c_{n-1} \in K$. Plugging in x results in the equation

$$0 = c_0 + c_1x + \dots + c_{n-1}x^{n-1} + x^n.$$

We may assume that $c_0 \neq 0$ (otherwise, we can multiply through by a suitable power of x^{-1} and reindex). Solving the above equation for c_0 and multiplying through by c_0^{-1} , we get

$$1 = -c_0^{-1}x^n - c_0^{-1} \sum_{i=1}^{n-1} c_i x^i.$$

The expression on the right belongs to the K -subspace S , since all positive powers of x lie in S (this follows from the equation $\langle SR \rangle = S$ and the fact that $x \in S \cap R$). Thus $1 \in S \subseteq A$, a contradiction. The claim is proved.

We now compute

$$\begin{aligned} \dim A &\geq \dim(S + (R \cap A)) \\ &= \dim S + \dim(R \cap A) - \dim(S \cap (R \cap A)) \\ &= \dim S + \dim(R \cap A) - \dim(S \cap R) \\ &= \dim S + \dim(R \cap A), \end{aligned}$$

where the last equality follows from the claim. This gives us

$$\dim S \leq \dim(A/(R \cap A)).$$

By Theorem ??, A is matched to itself.

The converse was discussed in Remark ??. □

Another consequence of Theorem ?? is a characterization of field extensions with respect to the linear matching property (see Section ?? to recall the definition). The corollary below is the commutative case of Theorem 2.6 in [?]. It can be viewed as a linear analogue of Corollary ??.

Corollary 3.6. *A field extension $K \subsetneq L$ has the linear matching property if and only if L contains no nontrivial proper finite-dimensional extension over K .*

Proof. Assume that L contains no nontrivial proper finite-dimensional extension over K . Let A and B be two n -dimensional K -subspaces of L , with $n > 0$ and $1 \notin B$. We aim to show that A is matched to B using Theorem ??.

To that end, suppose $S \subseteq A$ and $R \subseteq B \oplus K$ are nonzero K -subspaces such that $\langle SR \rangle = S$.

We claim that $R = K$. To see this, assume the contrary and let $x \in R \setminus K$. By Lemma ??, $[K(x) : K] \leq n$. Since $x \notin K$ and L contains no nontrivial proper finite-dimensional extension over K , it follows that $K(x) = L$. Hence

$$\dim L = [K(x) : K] \leq n.$$

Since $\dim B = n$, we must have $B = L$, contradicting $1 \notin B$. The claim is established.

Now observe that $R \cap B = \{0\}$, by the claim and the fact that $1 \notin B$. Hence

$$\dim S \leq \dim A = \dim B = \dim(B/(R \cap B)).$$

We now apply Theorem ?? to conclude that A is matched to B .

Conversely, assume that $K \subseteq L$ admits a nontrivial proper finite-dimensional extension over K . Then there exists an element $a \in L$ of finite degree $n \geq 2$ over K such that $K(a) \subsetneq L$. Choose an element $x \in L \setminus K(a)$, and define the K -subspaces A and B of L by

$$\begin{aligned} A &= \langle 1, a, a^2, \dots, a^{n-1} \rangle, \\ B &= \langle x, a, a^2, \dots, a^{n-1} \rangle. \end{aligned}$$

We will use Theorem ?? to show that A is not matched to B . Take $S = A$ and $R = \langle a, a^2, \dots, a^{n-1} \rangle$. Then $\langle SR \rangle = S$ (note that $A = K(a)$).

However, we have

$$\dim S = n > 1 = \dim(B/(R \cap B)),$$

violating the condition of Theorem ?. Therefore, A is not matched to B , implying that the field extension $K \subseteq L$ does not have the linear matching property. \square

Our final objective is to use Theorem ?? to establish the following linear counterpart to Corollary ??.

Corollary 3.7. *Let $K \subsetneq L$ be a field extension, and let $A, B \subseteq L$ be n -dimensional K -subspaces of L , with $n > 0$ and $1 \notin B$. Assume that for every $a \in L$ and every nontrivial proper finite-dimensional intermediate subfield $K \subseteq H \subseteq L$, the following inequality holds:*

$$\dim(aH \cap A) + \dim(H \cap B) < [H : K] + 1.$$

Then A is matched to B .

Proof. As usual, we assume $S \subseteq A$ and $R \subseteq B \oplus K$ are nonzero subspaces such that $\langle SR \rangle = S$. To apply Theorem ??, we need to show that

$$\dim S \leq \dim(B/(R \cap B)).$$

We claim that $R = K$. Assume the contrary, and let $x \in R \setminus K$. Let $a \in S \setminus \{0\}$. Applying Lemma ??, we find that $[K(x) : K] \leq n$ and $aK(x) \subseteq S$. Clearly $[K(x) : K] > 1$, as well. Note that $K(x) \neq L$, since otherwise, as in the previous proof, we would have $B = L$, contradicting $1 \notin B$. We now apply our hypothesis (taking $H = K(x)$), to obtain

$$\dim(aK(x) \cap A) + \dim(K(x) \cap B) < [K(x) : K] + 1.$$

Since $aK(x) \subseteq S \subseteq A$, this simplifies to

$$\dim K(x) + \dim(K(x) \cap B) < [K(x) : K] + 1,$$

forcing $\dim(K(x) \cap B) < 1$. But this is impossible, since $x \in R \setminus K$ and $R \subseteq B \oplus K$. The claim is proved.

By the claim and the fact that $1 \notin B$, we have $R \cap B = \{0\}$, so the inequality $\dim S \leq \dim(B/(R \cap B))$ holds trivially. Applying Theorem ?? completes the proof. \square

Remark 3.8. It seems plausible that Theorems ?? and ?? admit extensions to the non-commutative setting. Possible approaches include the use of Kemperman's d -transform (see [?]) along with its linearization as presented in [?]. Hamidoune's isoperimetric method [?] may also provide a viable framework for pursuing a generalization in the group setting.

Data sharing: Data sharing not applicable to this article as no datasets were generated or analysed.

Conflict of interest: To our best knowledge, no conflict of interests, whether of financial or personal nature, has influenced the work presented in this article.

References

- [1] M. Aliabadi. Conditions for matchability in groups and field extensions II. *Discuss. Math. Gen. Algebra Appl.* 45(1) (2025), 135–157.
- [2] M. Aliabadi, M. V. Janardhanan. On local matching property in groups and vector spaces. *Australas. J. Combin.* 70(1) (2018), 75–85.
- [3] M. Aliabadi, P. Taylor. Classifying abelian groups through acyclic matchings. *Ann. Combin.*, to appear.
- [4] M. Aliabadi, S. Zerbib. Matchings in matroids over abelian groups. *J. Algebraic Combin.* 59 (2024), 761–785.
- [5] N. Alon, C. K. Fan, D. Kleitman, J. Losonczy. Acyclic matchings. *Adv. Math.* 122(2) (1996), 234–236.
- [6] S. Eliahou, C. Lecouvey. Matchings in arbitrary groups. *Adv. Appl. Math.* 40 (2008), 219–224.
- [7] S. Eliahou, C. Lecouvey. Matching subspaces in a field extension. *J. Algebra* 324 (2010), 3420–3430.
- [8] S. Eliahou, C. Lecouvey. On linear versions of some addition theorems. *Linear Multilinear Algebra* 57 (2009), 759–775.
- [9] C. K. Fan, J. Losonczy. Matchings and canonical forms for symmetric tensors. *Adv. Math.* 117 (1996), no. 2, 228–238.
- [10] Y. O. Hamidoune. An isoperimetric method in additive theory. *J. Algebra* 179(2) (1996), 622–630.
- [11] Y. O. Hamidoune. Counting certain pairings in arbitrary groups. *Combin. Probab. Comput.* 20 (2011), no. 6, 855–865.
- [12] V. F. Lev. Small doubling in groups with moderate torsion. *SIAM J. Discrete Math.* 36 (2022), no. 1, 315–335.
- [13] J. Losonczy. On matchings in groups. *Adv. Appl. Math.* 20 (1998), no. 3, 385–391.
- [14] L. Lovász, M. D. Plummer. *Matching Theory*. Reprint of 1986 original, AMS Chelsea Publishing, 2009.
- [15] M. B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Springer-Verlag, New York, Berlin, Heidelberg, 1996.
- [16] J. E. Olson. On the sum of two sets in a group. *J. Number Theory* 18 (1984), 110–120.
- [17] R. Rado. A theorem on independence relations. *Quart. J. Math. Oxford Ser.* 13 (1942), 83–89.
- [18] E. K. Wakeford. On canonical forms. *Proc. London Math. Soc.* (2) 18 (1920), 403–410.