HAL open science

On linear versions of some addition theorems

Shalom Eliahou, Cédric Lecouvey

To cite this version:

Shalom Eliahou, Cédric Lecouvey. On linear versions of some addition theorems. 2008. hal-00258658

HAL Id: hal-00258658

https://hal.science/hal-00258658v1

Preprint submitted on 23 Feb 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

hal-00258658, version 1 - 23 Feb 2008

On linear versions of some addition theorems

Shalom Eliahou and Cédric Lecouvey
LMPA Joseph Liouville, FR CNRS 2956
Université du Littoral Côte d'Opale
50 rue F. Buisson, B.P. 699
F-62228 Calais cedex, France

Abstract

Let $K \subset L$ be a field extension. Given K-subspaces A, B of L, we study the subspace $\langle AB \rangle$ spanned by the product set $AB = \{ab \mid a \in A, b \in B\}$. We obtain some lower bounds on $\dim_K \langle AB \rangle$ and $\dim_K \langle B^n \rangle$ in terms of $\dim_K A$, $\dim_K B$ and n. This is achieved by establishing linear versions of constructions and results in additive number theory mainly due to Kemperman and Olson.

1 Introduction

Let G be a group, written multiplicatively. Given subsets $A, B \subset G$, we denote by

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

the *product set* of A, B. For A, B finite, several results in additive number theory give estimates on the cardinality of AB as a function of $|A|, |B|$. Instances of such results are the Cauchy-Davenport theorem for cyclic groups of prime order, a theorem of Kneser for abelian groups, and theorems of Kemperman and of Olson for possibly nonabelian groups.

In this paper, we consider the following analogous question. Given a field extension $K \subset L$, and finite-dimensional K-subspaces A, B of L, define

$$\langle AB \rangle = \text{ the } K\text{-subspace spanned by the product set } AB \text{ in } L.$$

What can be said, then, about the dimension of the subspace $\langle AB\rangle$? The main object of this paper is to establish linear analogues, in this new setting, of several results in additive number theory. In particular, we shall obtain nontrivial lower bounds on $\dim\langle AB\rangle$ in terms of $\dim A$, $\dim B$.

This question has barely been addressed in the literature. What seems to be the so far unique result of this type is due to Hou, Leung and Xiang [1] and is given below. We first recall Kneser's theorem from additive number theory [3, 4].

Theorem 1.1 (Kneser) *Let G be an abelian group and let $A, B \subset G$ be finite nonempty subsets. Then*

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

where $H = \{g \in G \mid gAB = AB\}$ is the stabilizer of AB.

The following linear version has been obtained in [1], and has motivated us to further explore the links between additive number theory, linear algebra and field extensions.

Theorem 1.2 (Hou, Leung and Xiang) *Let $K \subset L$ be a commutative field extension, and let $A, B \subset L$ be nonzero finite-dimensional K-subspaces of L. Suppose that every algebraic element in L is separable over K. Let H be the subfield of L which stabilizes $\langle AB\rangle$. Then*

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

The paper is organized as follows. Several classical results and constructions in additive number theory are recalled in Section 2. In Section 3, we give a new variant of a theorem of Olson. The switch to the field extension setting is performed from Section 4 on, where we give linear analogues of the additive results stated in the preceding sections.

2 Classical addition theorems

2.1 A basic result

One of the simplest results on the product of two sets in a finite group is the following. Given a subset X of a group G, we denote $X^{-1} = \{x^{-1} \mid x \in X\}$.

Proposition 2.1 *Let G be a finite group. Let A, B be nonempty subsets of G. If $|A| + |B| > |G|$, then $AB = G$.*

The proof, informally, goes as follows. For $x \in G$, we have $A^{-1}x \cap B \neq \emptyset$, since $|A^{-1}x| + |B| = |A| + |B| > |G|$. It follows that $x \in AB$.

Linearizing this result requires a little more work. This is done in Section 6, with various proofs.

2.2 Theorems of Kemperman and Olson

Here are a few classical results in additive number theory, to be linearized in subsequent sections. We refer the reader to [5] for proofs.

Theorem 2.2 (Kemperman) *Let A, B be two finite subsets of a group G. Assume there exists an element $c \in AB$ appearing exactly once as a product $c = ab$ with $a \in A$, $b \in B$. Then*

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

The next result is a nonabelian analogue of Kneser's Theorem 1.1.

Theorem 2.3 (Olson) *Let A, B be two finite subsets of a group G. There exists a nonempty subset S of AB and a finite subgroup H of G such that*

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

and either $HS = S$ or $SH = S$.

Here is an immediate corollary.

Theorem 2.4 (Kemperman) *Let G be a torsion-free group. Let A, B be nonempty finite subsets of G. Then*

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

Olson [5] also derived, as a consequence of Theorem 2.2 and 2.3, the following two interesting results. Linear versions are given in Section 9.

Theorem 2.5 (Olson) *Let A, B be finite subsets of a group G with $1 \in B$. Then*

$$AB^2 = AB \quad \text{or} \quad |AB| \geq |A| + \frac{1}{2}|B|.$$

Theorem 2.6 (Olson) *Let B be a finite subset of a group G. Then*

$$|B^n| = \left|B^{n+1}\right| \quad \text{or} \quad |B^n| \geq \left|B^{n-1}\right| + \frac{1}{2}|B|.$$

2.3 A main tool: the Kemperman transform

The above results are obtained by cleverly iterating Kemperman transforms, which we now recall.

Let G be a (possibly nonabelian) multiplicative group and (A, B) a pair of nonempty finite subsets of G. Let x be any element in G. The Kemperman transformed pairs (A', B') and (A'', B'') with respect to x are defined by

$$(A' = A \cup Ax,\ B' = B \cap x^{-1}B)$$

and

$$(A'' = A \cap Ax^{-1},\ B'' = B \cup xB).$$

The following properties are straightforward to check.

1. $A'B' \subset AB$ and $A''B'' \subset AB$;
2. $B' \neq \emptyset \iff x \in BB^{-1}$ and $A'' \neq \emptyset \iff x \in A^{-1}A$;
3. $|A'| > |A| \iff Ax \neq A$ and $|B''| > |B| \iff xB \neq B$.

Proposition 2.7 (Kemperman [2]) *Let (A, B) be a pair of nonempty finite subsets in a group G. Assume that there is an element $d \in A^{-1}A \cap BB^{-1}$ such that either $Ad \neq A$ or $dB \neq B$. Then there is a pair of nonempty subsets (A_1, B_1), obtained as a Kemperman transform of (A, B), satisfying:*

(1) $A_1B_1 \subset AB$,

(2) either $|A_1|+|B_1| = |A|+|B|$ *and* $|A_1| > |A|$, *or* $|A_1|+|B_1| > |A|+|B|$.

3 A variant of a theorem of Olson

In this section we give a variant of Theorem 2.5 which is neither stronger nor weaker, in the sense that neither result implies the other one. A linearized version of this variant will be presented in Section 8.

Theorem 3.1 *Let A, B, C be nonempty finite subsets of a group G. Suppose $B \subset C$ and $1 \in C$. Then*

$$ABC = AB \quad or \quad |ABC| \geq |A| + |B|.$$

Proof. The proof is close to that of Theorem 2.5 in [5]. If $C = \{1\}$ then $ABC = AB$. We now assume $|C| \geq 2$ and proceed by induction on $|AB|$.

If $|AB| = 1$ then $|A| = |B| = 1$, and $|ABC| = |C| \geq 2 \geq |A| + |B|$.

Assume now $|AB| > 1$ and our statement true for any pair (A_1, B_1) such that $B_1 \subset C$ and $|A_1B_1| < |AB|$. As in Olson's original proof of Theorem 2.5, we consider two cases.

(i) Assume there exists a nonempty subset $S \subset AB$ such that $SC = S$. Since S is finite, we have $Sc = S$ for all $c \in C$, whence $SC^{-1} = S$.

Set $A_0 = A \cap S$ and $A_1 = A \setminus S$, so that $A = A_0 \sqcup A_1$. We claim that

$$A_0B = S. \tag{1}$$

Indeed, as $B \subset C$, we have $A_0B \subset SC = S$. Conversely, let $s \in S$. Then $s = ab$ for some $a \in A$ and $b \in B$. Since $a = sb^{-1} \in SC^{-1} = S$, it follows that $a \in A_0$, whence $s \in A_0B$ as desired.

As a first consequence, we obtain

$$AB = S \sqcup A_1B. \tag{2}$$

Indeed, we have $AB = A_0B \cup A_1B = S \cup A_1B$. Moreover, as $S \cap A_1 = \emptyset$, we have $SB^{-1} \cap A_1 = \emptyset$ since $SB^{-1} \subset SC^{-1} = S$. It follows that $S \cap A_1B = \emptyset$.

Our next claim is that

$$ABC = S \sqcup A_1BC. \tag{3}$$

Indeed, we have $ABC = SC \cup A_1BC = S \cup A_1BC$. The intersection $S \cap A_1BC$ is indeed empty, since $S = SC^{-1}$ and so $SC^{-1} \cap A_1B = S \cap A_1B = \emptyset$.

Consequently, we derive

$$|ABC| \geq |S| + |A_1BC| \geq |A_0| + |A_1BC|, \tag{4}$$

where the estimate $|S| \geq |A_0|$ follows from the equality $S = A_0B$ in (1).

We may assume $A_1 \neq \emptyset$, for otherwise $S = A_0B = AB$, whence $ABC = SC = S = AB$ and we are done. We have $|A_1B| < |AB|$ by (2). By our induction hypothesis, we either have $A_1BC = A_1B$ or $|A_1BC| \geq |A_1| + |B|$.

If $A_1BC = A_1B$, then by (3) and (2), we obtain $ABC = S \cup A_1BC = S \cup A_1B = AB$ and we are done in this case.

If now $|A_1BC| \geq |A_1| + |B|$, then by (4) and $|A| = |A_0| + |A_1|$, we get

$$|ABC| \geq |A_0| + |A_1BC| \geq |A_0| + |A_1| + |B| = |A| + |B|,$$

and we are done in this case as well.

(ii) Assume now $XC \neq X$ for every nonempty subset $X \subset AB$.

By Theorem 2.3, there exists a nonempty subset $S \subset AB$ and a subgroup H such that

$$|S| \geq |A| + |B| - |H| \tag{5}$$

and $HS = S$ or $SH = S$. Let $c_0 \in C$ be such that $Sc_0 \neq S$. We claim that

$$|S \cup Sc_0| \geq |S| + |H|. \tag{6}$$

Indeed, if $HS = S$, then $H(S \cup Sc_0) = S \cup Sc_0$, and hence $S \cup Sc_0$ is a disjoint union of left cosets of H. This implies (6) in this case.

On the other hand, if $SH = S$, pick $s_0 \in S$ such that $s_0c_0 \notin S$, and set $H' = H \cup \{c_0\}$. In the set SH', the element s_0c_0 appears exactly once, since $SH \subset S$. Applying Theorem 2.2, it follows that

$$|SH'| \geq |S| + |H'| - 1 = |S| + |H|\,. \tag{7}$$

This implies (6) again, since $SH' = S \cup Sc_0$.

Now, as $\{1, c_0\} \subset C$, we have $S \cup Sc_0 \subset SC$, and therefore

$$|ABC| \geq |SC| \geq |S \cup Sc_0|\,.$$

Combined with (5) and (6), this gives

$$|ABC| \geq |S| + |H| \geq |A| + |B|\,.$$

■

In the abelian case, the previous theorem is much shorter to prove, using Kneser's theorem, and remains true without the assumption $B \subset C$.

Theorem 3.2 *Let A, B, C be nonempty finite subsets of an abelian group G. Suppose $1 \in C$. Then*

$$ABC = AB \quad \textit{or} \quad |ABC| \geq |A| + |B|\,.$$

Proof. By Kneser's theorem, we obtain

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

where H is the stabilizer of AB in G. We have $HAB = AB$ and hence $HABC = ABC$. In particular, both AB and ABC are disjoint unions of cosets of H. We have $AB \subset ABC$ since $1 \in C$. Therefore, if $ABC \neq AB$, it follows from the above that

$$|ABC| \geq |AB| + |H| \geq |A| + |B|\,.$$

■

4 The linear setting

From now on, and for the remainder of this paper, K is a commutative field and L a (possibly skew) field extension containing K in its center. Given any subset $S \subset L$, we write $\langle S \rangle$ for the K-subspace of L generated by S. For subsets S_1, S_2 of L, we consider the product set

$$S_1 S_2 = \{s_1 s_2 \mid s_1 \in S_1, s_2 \in S_2\}$$

and the K-subspace $\langle S_1 S_2 \rangle$ of L spanned by $S_1 S_2$. Note, for later use, the equality

$$\langle\, \langle S_1 \rangle \langle S_2 \rangle \,\rangle = \langle S_1 S_2 \rangle.$$

If $S_1 = \{x\}$, we simply write xS_2 instead of $\{x\}S_2$. When $S_1 = A$, $S_2 = B$ are finite-dimensional K-subspaces of L, it is easy to verify that $\langle AB \rangle$ is finite-dimensional, with

$$\dim_K \langle AB \rangle \leq (\dim_K A)(\dim_K B).$$

Also, for any nonzero $x \in L$, the sets xA and Ax are K-subspaces of L, with $\dim_K(xA) = \dim_K(Ax) = \dim_K A$.

Notation. For any subset $X \subset L$, we denote $X_* = X \setminus \{0\}$ and

$$X_*^{-1} = \{x^{-1} \mid x \in X_*\},$$

the set of inverses of the nonzero elements of X.

Note that $X_*^{-1} \cup \{0\}$ is not a K-subspace of L in general, even if X is.

In subsequent sections we establish linear versions of the addition theorems recalled above. In particular, we obtain lower bounds on $\dim_K \langle AB \rangle$ in terms of $\dim_K A$, $\dim_K B$. As for the groups setting, our main tool will be a linear version of the Kemperman transform.

5 A linear Kemperman transform

Let (A, B) be a pair of finite-dimensional K-subspaces of L. Let $x \in L \setminus \{0\}$. We define the transformed pairs (A', B') and (A'', B'') with respect to x as follows:

$$(A' = A + Ax,\ B' = B \cap x^{-1}B)$$

and

$$(A'' = A \cap Ax^{-1},\ B'' = B + xB),$$

where $+$ denotes the usual sum of vector subspaces. Since $A+Ax = \langle A \cup Ax \rangle$, we may view them as linear analogues of the classical Kemperman transforms. (Compare with Section 2.3.) They satisfy the analogous properties below:

1. A', B', A'', B'' are K-vector subspaces of L,
2. $\langle A'B' \rangle \subset \langle AB \rangle$ and $\langle A''B'' \rangle \subset \langle AB \rangle$,
3. $B' \neq \{0\} \iff x \in BB_*^{-1}$ and $A'' \neq \{0\} \iff x \in A_*^{-1}A$,
4. $\dim_K A' > \dim_K A \iff Ax \neq A$ and
   $\dim_K B'' > \dim_K B \iff xB \neq B$.

Proposition 5.1 *With the same notation as above, set $D = A_*^{-1}A \cap BB_*^{-1}$. Suppose that either $AD \not\subset A$ or $DB \not\subset B$. Then there exists a pair (A_1, B_1) of K-subspaces of L satisfying:*

(1) $A_1 \neq \{0\}$ *and* $B_1 \neq \{0\}$,

(2) $\langle A_1B_1 \rangle \subset \langle AB \rangle$,

(3) either $\dim_K A_1 + \dim_K B_1 = \dim_K A + \dim_K B$ *and* $\dim_K A_1 > \dim_K A$, *or* $\dim_K A_1 + \dim_K B_1 > \dim_K A + \dim_K B$.

Point (3) above looks somewhat technical, but it has a very interesting and useful meaning. It says that, in $\mathbb{N}^2$ ordered lexicographically, one has

$$\big(\dim_K A_1 + \dim_K B_1,\ \dim_K A_1\big) > \big(\dim_K A + \dim_K B,\ \dim_K A\big).$$

This is used, for instance, in the proof of Corollary 5.2 below. Here again, note that the set $D = A_*^{-1}A \cap BB_*^{-1}$ needs not be a K-subspace of L.

Proof. Since $AD \not\subset A$ or $DB \not\subset B$, there is an element $d \neq 0$ in D such that $Ad \not\subset A$ or $dB \not\subset B$. Denote p, q the dimensions of the following quotient spaces:

$$p = \dim_K (A + Ad)/A, \quad q = \dim_K (B + dB)/B.$$

We have $\max(p, q) \geq 1$, and we need to distinguish two cases.

• Assume first $p \geq q$. In this case, we make the linear Kemperman transform

$$A_1 = A + Ad, \quad B_1 = B \cap d^{-1}B.$$

We have $A \subsetneq A_1$ since $p \geq 1$, and $B_1 \neq \{0\}$ since $d \in D \subset BB_*^{-1}$. Moreover $\langle A_1 B_1 \rangle \subset \langle AB \rangle$. This settles the first two requirements on (A_1, B_1). As for the third one, we claim that

$$\dim_K A_1 = \dim_K A + p, \quad \dim_K B_1 = \dim_K B - q.$$

Indeed, our definitions imply $p = \dim_K A_1 - \dim_K A$, and we have

$$\begin{aligned} \dim_K B_1 &= \dim_K (B \cap d^{-1}B) \\ &= \dim_K (dB \cap B) \\ &= \dim_K dB + \dim_K B - \dim_K (dB + B) \\ &= \dim_K B - q. \end{aligned}$$

It follows that

$$\dim_K A_1 + \dim_K B_1 = \dim_K A + \dim_K B + p - q,$$

whence $\dim_K A_1 + \dim_K B_1 \geq \dim_K A + \dim_K B$, and $\dim_K A_1 > \dim_K A$ since $p \geq 1$. This yields the third requirement on (A_1, B_1).

• Assume now $p < q$. Here we use the other linear Kemperman transform and set

$$A_1 = A \cap Ad^{-1}, \quad B_1 = B + dB.$$

This time we have $B \subsetneq B_1$ since $q \geq 1$, and $A_1 \neq \{0\}$ since $d \in D \subset A_*^{-1}A$. We have $\langle A_1 B_1 \rangle \subset \langle AB \rangle$, and a similar calculation as above yields

$$\dim_K A_1 = \dim_K A - p, \quad \dim_K B_1 = \dim_K B + q.$$

It follows that

$$\dim_K A_1 + \dim_K B_1 = \dim_K A + \dim_K B + q - p,$$

implying $\dim_K A_1 + \dim_K B_1 > \dim_K A + \dim_K B$, as desired. ■

Corollary 5.2 *Let A, B be nonzero finite-dimensional K-subspaces of L. Then there exist nonzero finite-dimensional K-subspaces E, F of L satisfying*

(1) $\langle EF\rangle \subset \langle AB\rangle$,

(2) $\dim_K E + \dim_K F \geq \dim_K A + \dim_K B$,

(3) $ED = E$ *and* $DF = F$, *where* $D = E_*^{-1}E \cap FF_*^{-1}$.

Proof. By successive applications of the previous proposition, we get a sequence

$$(A, B) = (A_0, B_0), (A_1, B_1), \ldots, (A_i, B_i), \ldots$$

of pairs of K-subspaces of L satisfying the following properties, for $i \geq 1$:

- $\langle A_iB_i\rangle \subset \langle A_{i-1}B_{i-1}\rangle$,
- $\big(\dim_K A_i + \dim_K B_i,\ \dim_K A_i\big) > \big(\dim_K A_{i-1} + \dim_K B_{i-1},\ \dim_K A_{i-1}\big)$ in $\mathbb{N}^2$ ordered lexicographically.

Moreover, these spaces have bounded dimension, since

$$\begin{aligned} \max\{\dim_K A_i, \dim_K B_i\} &\leq \dim_K\langle A_iB_i\rangle \\ &\leq \dim_K\langle AB\rangle \\ &\leq (\dim_K A)(\dim_K B). \end{aligned}$$

It follows that the above sequence must be finite. By Proposition 5.1, there is an index $n \geq 0$ such that the set $D = (A_n)_*^{-1}A_n \cap B_n(B_n)_*^{-1}$ satisfies $A_nD \subset A_n$ and $DB_n \subset B_n$. In fact $A_nD = A_n$ and $DB_n = B_n$, since $1 \in D$. Setting $E = A_n$, $F = B_n$, it follows from the properties of the sequence of (A_i, B_i) that $\langle EF\rangle \subset \langle AB\rangle$ and $\dim_K E + \dim_K F \geq \dim_K A + \dim_K B$. ■

6 Linearizing Theorem 2.3 of Olson

With the linearized Kemperman transform at hand, we are now ready to establish linear versions of the addition theorems of Section 2 and 3. We start with Theorem 2.3 of Olson. The following easy lemma will be needed in the process.

Lemma 6.1 *Let D be a finite-dimensional K-subspace of L. Then D is a (possibly skew) field if and only if* $1 \in D$ *and* $D^2 \subset D$.

Proof. It suffices to show that every nonzero element $d \in D$ is invertible in D. Now the map $L_d : D \to D$ defined by $L_d(x) = dx$ for all $x \in D$, is linear and injective. Hence L_d is bijective, and therefore there is some $d' \in D$ with $L(d') = 1$. Obviously d' is the inverse of d in L and it does live in D. ■

Theorem 6.2 *Let K be a commutative field and L a field extension of K. Let A, B be finite-dimensional K-vector spaces in L distinct from $\{0\}$. Then there exist a K-vector subspace S of $\langle AB \rangle$ and a subfield H of L such that*

(1) $K \subset H \subset L$,

(2) $\dim_K S \geq \dim_K A + \dim_K B - \dim_K H$,

(3) $HS = S$ *or* $SH = S$.

Proof. By Corollary 5.2, there are subspaces E, F such that

$$\langle EF \rangle \subset \langle AB \rangle, \quad \dim_K E + \dim_K F \geq \dim_K A + \dim_K B,$$

and $ED = E$, $DF = F$ where $D = E_*^{-1}E \cap FF_*^{-1}$.

We start by assuming $\dim_K E \geq \dim_K F$ and, as in the proof of Olson's theorem, we distinguish two cases:

(i) $FF_*^{-1} \not\subset E_*^{-1}E$. Then there exist $x_1, x_2 \in F_*$ such that $x_1x_2^{-1} \notin E_*^{-1}E$. Therefore $Ex_1 \cap Ex_2 = \{0\}$ and $Ex_1 \oplus Ex_2 \subset \langle EF \rangle$. This gives $\dim_K \langle EF \rangle \geq 2\dim_K E \geq \dim_K E + \dim_K F$. Let $H = K$ and $S = \langle EF \rangle$. Then H is a subfield of L stabilizing S, and $\dim_K \langle S \rangle \geq \dim_K A + \dim_K B - 1$, as desired.

(ii) $FF_*^{-1} \subset E_*^{-1}E$. Then $D = FF_*^{-1}$ and $1 \in D$. Moreover, we have

$$DD = DFF_*^{-1} = FF_*^{-1} = D$$

since $DF = F$. So $D^2 \subset D$. Let z be a nonzero element of F. We have

$$F = Fz^{-1}z \subset Dz \subset DF = F$$

because $Fz^{-1} \subset D$ and $DF = F$. This implies that $Dz = F$ and thus $D = Fz^{-1}$ is a finite-dimensional K-vector space in L. Since $1 \in D$ and $D^2 = D$, we derive from Lemma 6.1 that D is a subfield of L containing K. Moreover $\dim_K D = \dim_K F$. Set $S = \langle EF \rangle$ and $H = z^{-1}Dz$. Since D is a field, H is also a field and $\dim_K H = \dim_K D = \dim_K F$. We have

$$SH \subset \langle EFH \rangle = \langle EFz^{-1}Dz \rangle = \langle EDzz^{-1}Dz \rangle = \langle EDz \rangle = \langle EF \rangle = S$$

since $Dz = F$ and $D^2 = D$. It follows that $SH = S$. We have $\dim_K S = \dim_K \langle EF \rangle \geq \dim_K E$ since $F \neq \{0\}$. Finally, this gives

$$\dim_K S \geq \dim_K E + \dim_K F - \dim_K H$$

because $\dim_K H = \dim_K D = \dim_K F$.

This settles the case $\dim_K E \geq \dim_K F$. The case $\dim_K F \geq \dim_K E$ can be treated in a similar way. ■

Remarks.

(i) In contrast to the linear version of Kneser's Theorem 1.2, our linear version of Olson's Theorem does not require any separability hypothesis.

(ii) Assume that L is commutative and $\dim_K L = p$, a prime number. In that case, there is no intermediate field $K \subset H \subset L$ besides K, L. It follows from the above theorem that either $\langle AB \rangle = L$ or $\dim_K \langle AB \rangle \geq \dim_K S \geq \dim_K A + \dim_K B - 1$. This is also a consequence of Theorem 1.2, provided L is further assumed to be separable over K.

(iii) Suppose that K is a finite field of cardinality q. Then $A^* = A \backslash \{0\}$ and $B^* = B \backslash \{0\}$ are finite subsets of the group $L^* = L \backslash \{0\}$, and by Theorem 2.3, there exist a subset $\mathcal{S}^*$ of $A^* B^*$ and a subgroup $\mathcal{H}^*$ of L^* such that

$$|\mathcal{S}^*| \geq |A^*| + |B^*| - |\mathcal{H}^*| \,.$$

Thus, we get

$$|A| + |B| \leq |\mathcal{S}^*| + |\mathcal{H}^*| + 2.$$

However, with Theorem 6.2, we obtain

$$q^{\dim_K A} q^{\dim_K B} \leq q^{\dim_K S} q^{\dim_K H},$$

and since $|K| = q$, this gives

$$|A| \, |B| \leq |S| \, |H| \,.$$

Thus, Theorem 2.3 gives an upper bound for $|A|+|B|$, whereas Theorem 6.2 gives an upper bound for $|A| \, |B|$. Note that $\mathcal{S}^* \neq S \backslash \{0\}$ and $\mathcal{H}^* \neq H \backslash \{0\}$ in general.

One first easy consequence is a linear version of Kemperman's Theorem 2.4 on torsion-free groups.

Theorem 6.3 *Let K be a commutative field and L a (possibly skew) purely transcendental extension of K. Let A, B be nonzero finite-dimensional K-subspaces of L. Then*

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

Proof. By Theorem 6.2, there is a subspace $S \subset \langle AB \rangle$ and an intermediary field $K \subset H \subset L$ such that

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

and $HS = S$ or $SH = S$. As $\dim_K S$ is finite, it follows that $\dim_K H$ must be finite as well. But K is the only finite-dimensional subfield of L. It follows that $H = K$ and hence $\dim_K H = 1$. ■

Remark. The above lower bound is sharp. Indeed, let $x \in L \setminus K$. Then x is transcendental over K. Fix positive integers r, s. Let A, B be the subspaces of L generated by $\{1, x, \ldots, x^{r-1}\}$, $\{1, x, \ldots, x^{s-1}\}$, respectively. Then $\dim_K A = r$, $\dim_K B = s$ and $\dim_K \langle AB \rangle = r + s - 1$, since $\langle AB \rangle$ is the subspace spanned by the basis $\{1, x, \ldots, x^{r+s-2}\}$.

We now derive, from Theorem 6.2 again, a linear version of the basic Proposition 2.1.

Proposition 6.4 *Let K be a commutative field and L a field extension containing K in its center, with $\dim_K L$ finite. Let A, B be nonzero subspaces of L satisfying $\dim_K A + \dim_K B > \dim_K L$. Then $\langle AB \rangle = L$.*

Note that the hypothesis that L is a field is essential. For otherwise, a counterexample would be provided by $A = L$ and $B =$ a proper nonzero left ideal of L, yielding $\langle AB \rangle = B$.

Proof. By Theorem 6.2, there is a subspace $S \subset \langle AB \rangle$ and an intermediate field $K \subset H \subset L$ such that

$$\dim_K S \geq \dim_K A + \dim_K B - \dim_K H, \tag{8}$$

and either $HS = S$ or $SH = S$. We claim that $HS = L = SH$. Indeed, fix any nonzero element $x \in L$. It follows from (8) and the hypothesis $\dim_K A + \dim_K B > \dim_K L$, that

$$\dim_K S + \dim_K(xH) > \dim_K L.$$

Therefore $S \cap xH \neq \{0\}$. Hence, there are nonzero elements $s \in S$ and $h \in H$ such that $s = xh$. But then $x = sh^{-1}$ belongs to SH, since $h^{-1} \in H$. It follows that $L = HS$. The same argument, with xH replaced by Hx, yields $L = SH$. We conclude $L = S = \langle AB \rangle$, since $S \subset \langle AB \rangle$ and $S = HS$ or SH. ■

When L is commutative, the above result admits a much simpler proof, which does not require Theorem 6.2.

Proposition 6.5 *Let $K \subset L$ be a commutative field extension, with $\dim_K L$ finite. Let A, B be nonzero subspaces of L satisfying $\dim_K A + \dim_K B > \dim_K L$. Then $\langle AB \rangle = L$.*

Proof. We may assume $A, B \neq L$ and proceed by induction on $\dim_K B$. If $\dim_K B = 1$, then $\dim_K A = \dim_K L$ and $\langle AB \rangle = \langle LB \rangle = L$. Assume now $\dim_K B \geq 2$. Since $\langle LB \rangle = L$, there must be a nonzero element $x \in L$ such that $xB \not\subset A$. Set

$$A' = A + xB, \ B' = Ax^{-1} \cap B.$$

We have $A'B' \subset \langle AB \rangle$ by construction and the commutativity of L. Moreover, the subspace B' is nonzero, since $\dim_K Ax^{-1} + \dim_K B = \dim_K A + \dim_K B > \dim_K L$. Finally, $\dim_K A' + \dim_K B' = \dim_K A + \dim_K B$, since

$$\begin{aligned} \dim_K A' = \dim_K(A + xB) &= \dim_K A + \dim_K xB - \dim_K(A \cap xB) \\ &= \dim_K A + \dim_K B - \dim_K(Ax^{-1} \cap B) \\ &= \dim_K A + \dim_K B - \dim_K B'. \end{aligned}$$

By the induction hypothesis, we conclude $\langle A'B' \rangle = L = \langle AB \rangle$. ■

Remark. We are grateful to Joseph Oesterlé for providing us with the following alternative proof of Proposition 6.4, which only uses duality in vector spaces.

Proof. Let H be any hyperplane in L, and let $\varphi : L \to K$ be a linear form with kernel H. It suffices to show that there exist $a \in A$, $b \in B$ such that $\varphi(ab) \neq 0$, implying $\langle AB \rangle \not\subset H$.

The map $\beta : L \times L \to K$ defined by $\beta(x, y) = \varphi(xy)$ for all $x, y \in L$ is a K-bilinear form, and it is non-degenerate: if $x \neq 0$, then xL is equal to L and hence $\varphi(xL) \neq \{0\}$. Therefore β induces an isomorphism $\gamma : L \to L^*$, where L^* is the dual of L, defined by the formula $\gamma(x)(y) = \beta(x, y)$ for all $x, y \in L$.

From the inclusion map $j : B \to L$ we deduce, by transposition, a surjection $j^t : L^* \to B^*$, defined as usual by $j^t(\psi) = \psi \circ j$ for all $\psi \in L^*$. The composition $j^t \circ \gamma : L \to B^*$ is then also surjective, and therefore

$$\dim_K \ker(j^t \circ \gamma) = \dim_K L - \dim_K B < \dim_K A.$$

Thus, there is some $a \in A$ satisfying $j^t(\gamma(a)) \neq 0$. Since the linear form $\gamma(a) \circ j : B \to K$ does not vanish, there must be some $b \in B$ satisfying $\gamma(a)(b) \neq 0$, i.e. $\beta(a, b) = \varphi(ab) \neq 0$. ■

7 Linearizing Theorem 2.2 of Kemperman

We shall now establish a linear analogue of Kemperman's Theorem 2.2, according to which, for subsets A, B in a group G, one has $|AB| \geq |A| + |B| - 1$ provided there is an element $c \in AB$ with a *unique representation* of the form $c = ab$ with $a \in A, b \in B$.

In order to properly linearize this result, we need to rephrase the above unicity condition on c. First, up to translation of A, B, we may assume that $1 \in A \cap B$ and that $c = 1$ admits the unique representation $1 = ab$ with $a = b = 1$ as a product in AB. If we write

$$\begin{aligned} A &= \{1\} \sqcup \overline{A} \\ B &= \{1\} \sqcup \overline{B} \end{aligned}$$

with $\overline{A}, \overline{B}$ the respective complements of $\{1\}$ in A, B, then the unicity of 1 as a product in AB is equivalent to the disjointness condition

$$\{1\} \cap (\overline{A} \cup \overline{B} \cup \overline{A}\,\overline{B}) = \emptyset,$$

which may also be written as $AB = \{1\} \sqcup (\overline{A} \cup \overline{B} \cup \overline{A}\,\overline{B})$. These equivalent conditions motivate the following formulation of our sought-for linearization.

Theorem 7.1 *Let K be a commutative field and L a field extension of K. Let A, B be finite-dimensional K-vector spaces in L such that $K \subset A \cap B$. Suppose there exist subspaces $\overline{A}, \overline{B} \subset L$ such that*

$$A = K \oplus \overline{A},\ \ B = K \oplus \overline{B} \text{ and } K \cap (\overline{A} + \overline{B} + \langle \overline{A}\,\overline{B} \rangle) = \{0\}. \tag{9}$$

Then

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

Proof. Observe first that, if $A = K + \overline{A}$ and $B = K + \overline{B}$, then $\langle AB \rangle = K + (\overline{A} + \overline{B} + \langle \overline{A}\,\overline{B} \rangle)$. Therefore, condition (9) is equivalent to

$$A = K \oplus \overline{A},\ \ B = K \oplus \overline{B} \text{ and } \langle AB \rangle = K \oplus (\overline{A} + \overline{B} + \langle \overline{A}\,\overline{B} \rangle).$$

Since $1 \in A \cap B$, we have $A + B \subset \langle AB \rangle$. We now distinguish two cases.

Case 1. Assume $A \cap B = K$. Then $\dim_K (A + B) = \dim_K A + \dim_K B - 1$, and we are done since $\dim_K \langle AB \rangle \geq \dim_K (A + B)$.

Case 2. Assume now $A \cap B \neq K$, i.e. $\dim_K A \cap B \geq 2$. We first claim that

$$A \cap B = K \oplus (\overline{A} \cap \overline{B}). \tag{10}$$

Indeed, let $x \in A \cap B$. Then there are $\lambda, \mu \in K$ and $\overline{x} \in \overline{A}, \overline{y} \in \overline{B}$ such that

$$x = \lambda + \overline{x} = \mu + \overline{y}.$$

Since $K \cap (\overline{A} + \overline{B}) = \{0\}$, it follows that $\lambda = \mu$ and $\overline{x} = \overline{y}$, so that $x \in K \oplus (\overline{A} \cap \overline{B})$, as claimed. The reverse inclusion is immediate.

Observe that in the present case, we have $\overline{A} \cap \overline{B} \neq \{0\}$. We shall perform a suitable sequence of linear Kemperman transforms on the pair (A, B) and eventually reach Case 1 again, thereby concluding the proof.

Let $0 \neq d \in \overline{A} \cap \overline{B}$ be any nonzero element. We perform a Kemperman transform on (A, B) relative to d, and get a new pair (A_1, B_1), by defining either

$$(i) \quad A_1 = A + Ad, \quad B_1 = B \cap d^{-1}B, \text{ or} \tag{11}$$

$$(ii) \quad A_1 = A \cap Ad^{-1}, \quad B_1 = B + dB. \tag{12}$$

In either case, we have $\langle A_1 B_1 \rangle \subset \langle AB \rangle$, and one of (i) or (ii) will yield the estimate

$$\dim_K A_1 + \dim_K B_1 \geq \dim_K A + \dim_K B.$$

Case (i). For any nonzero element $d \in \overline{A} \cap \overline{B}$, define

$$\begin{aligned} A_1 &= A + Ad, \\ B_1 &= B \cap d^{-1}B. \end{aligned}$$

We shall show that this new pair satisfies the hypotheses of the theorem. Indeed, define

$$\begin{aligned} \overline{A_1} &= \overline{A} + Ad, \\ \overline{B_1} &= \overline{B} \cap d^{-1}\overline{B}. \end{aligned}$$

We claim that conditions (9) are satisfied, i.e.

$$A_1 = K \oplus \overline{A_1}, \tag{13}$$

$$B_1 = K \oplus \overline{B_1}, \tag{14}$$

$$\{0\} = K \cap (\overline{A_1} + \overline{B_1} + \langle \overline{A_1}\,\overline{B_1} \rangle). \tag{15}$$

For (13): We have $K + \overline{A_1} = K + \overline{A} + Ad = A + Ad = A_1$. The sum is direct, since $\overline{A_1} \subset \overline{A} + Kd + \overline{A}d \subset \overline{A} + \overline{B} + \langle \overline{A}\,\overline{B} \rangle$, whence $K \cap \overline{A_1} = \{0\}$ by (9).

For (14): To start with, we have $K \cap \overline{B_1} \subset K \cap \overline{B} = \{0\}$ by (9).

We next verify the inclusion $K + \overline{B_1} \subset B_1$. We have $K \subset B$, and $K \subset d^{-1}B$ since $d \in B$, whence $K \subset B_1$. Moreover, we have $\overline{B_1} = \overline{B} \cap d^{-1}\overline{B} \subset B \cap d^{-1}B = B_1$. This establishes the desired inclusion.

It remains to prove the reverse inclusion $B_1 \subset K + \overline{B_1}$. Let $x \in B_1 = B \cap d^{-1}B$. Since $B = K \oplus \overline{B}$, we may write $x = \lambda + \overline{x}$ for some $\lambda \in K$ and $\overline{x} \in \overline{B}$. It remains to show that $\overline{x} \in \overline{B_1} = \overline{B} \cap d^{-1}\overline{B}$, i.e. that $\overline{x} \in d^{-1}\overline{B}$. Since $x \in d^{-1}B$, there are elements $y \in B$, $\mu \in K$ and $\overline{y} \in \overline{B}$ such that $x = d^{-1}y$ and $y = \mu + \overline{y}$. Hence $dx = y$, and therefore

$$d\lambda + d\overline{x} = \mu + \overline{y}.$$

It follows that $\mu = d\lambda + d\overline{x} - \overline{y}$, whence $\mu \in K \cap (\overline{B} + \langle \overline{A}\,\overline{B} \rangle)$. Therefore $\mu = 0$ by (9), whence $d\overline{x} = \overline{y} - d\lambda \in \overline{B}$. This shows that $\overline{x} \in d^{-1}\overline{B}$, implying $\overline{x} \in \overline{B_1}$ and finally $x \in K + \overline{B_1}$, as desired.

For (15): By (9), it suffices to show the inclusion

$$(\overline{A_1} + \overline{B_1} + \langle \overline{A_1}\,\overline{B_1} \rangle) \subset (\overline{A} + \overline{B} + \langle \overline{A}\,\overline{B} \rangle).$$

Considering each summand at a time in the left-hand side, we have:
• $\overline{A_1} = \overline{A} + Ad = \overline{A} + Kd + \overline{A}d \subset (\overline{A} + \overline{B} + \langle \overline{A}\,\overline{B} \rangle)$,
• $\overline{B_1} = \overline{B} \cap d^{-1}\overline{B} \subset \overline{B}$,
• $\overline{A_1}\,\overline{B_1} = (\overline{A} + Ad)(\overline{B} \cap d^{-1}\overline{B}) \subset \overline{A}\,\overline{B} + A\,\overline{B} \subset \overline{A}\,\overline{B} + \overline{B} + \overline{A}\,\overline{B}$,
and we are done.

Case (ii). For any nonzero element $d \in \overline{A} \cap \overline{B}$, define

$$\begin{aligned} A_1 &= A \cap Ad^{-1}, \\ B_1 &= B + dB. \end{aligned}$$

This time, we set

$$\begin{aligned} \overline{A_1} &= \overline{A} \cap \overline{A}d^{-1}, \\ \overline{B_1} &= \overline{B} + dB. \end{aligned}$$

With arguments similar to those of Case (i), we can prove that conditions (9) are satisfied again, i.e.

$$\begin{aligned} A_1 &= K \oplus \overline{A_1}, \\ B_1 &= K \oplus \overline{B_1}, \\ \{0\} &= K \cap (\overline{A_1} + \overline{B_1} + \langle \overline{A_1}\,\overline{B_1} \rangle). \end{aligned}$$

Now, as in the proof of Corollary 5.2, we iterate the above Kemperman transforms as long as possible. At each step, we get new subspaces A_i, B_i satisfying (9) and such that

$$\big(\dim_K A_i + \dim_K B_i,\, \dim_K A_i\big) > \big(\dim_K A_{i-1} + \dim_K B_{i-1},\, \dim_K A_{i-1}\big)$$

in $\mathbb{N}^2$ ordered lexicographically. Since these subspaces have bounded dimension, the iteration cannot continue indefinitely and Case 1 must eventually be reached. This means that there exist subspaces E, F of L such that

$$\langle EF \rangle \subset \langle AB \rangle, \tag{16}$$

$$\dim_K E + \dim_K F \geq \dim_K A + \dim_K B, \tag{17}$$

and satisfying $E \cap F = K$ together with the hypotheses of the theorem. By Case 1, we have

$$\dim_K \langle EF \rangle \geq \dim_K E + \dim_K F - 1.$$

The desired inequality, namely

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

now follows from (16) and (17). ■

8 Linearizing Theorem 3.1

Throughout the last two sections, we shall assume that L is a commutative field extension of K and that every algebraic element of L is separable over K. This allows us to use Theorem 1.2, the linear version of Kneser's Theorem.

Our results below probably remain true in the more general setting of the preceding sections, where L is only assumed to be a field containing K in its center. But we have no proof of this so far.

Lemma 8.1 *Let K be a commutative field, H a field extension of K and L a field extension of H. Let V be a finite-dimensional K-vector space in L such that $HV = V$. Then there exists a finite subset $R_V \subset V$ such that*

$$V = \bigoplus_{v \in R_V} Hv. \tag{18}$$

In particular $\dim_K H$ *is finite and divides* $\dim_K V$.

Proof. For any $v \in V$, Hv is vector subspace of V. Moreover for any v, v' in V, one has $Hv = Hv'$ or $Hv \cap Hv' = \{0\}$. The lemma follows immediately since $\dim_K V$ is finite. ■

Remark. If $HV = V$, then V can be interpreted as a finite-dimensional left H-module, and (18) gives its decomposition into irreducible components.

We now give a linear version of Theorem 3.1. As mentioned above, the hypotheses on L are probably more restrictive than actually necessary.

Theorem 8.2 *Let $K \subset L$ be commutative fields such that every algebraic element in L is separable over K. Let $A, B, C \subset L$ be finite-dimensional K-subspaces of L such that $A, B \neq \{0\}$ and $K \subset C$. Then either*

$$\langle ABC \rangle = \langle AB \rangle \quad \textit{or} \quad \dim_K \langle ABC \rangle \geq \dim_K A + \dim_K B.$$

Proof. We shall apply Theorem 1.2. The stabilizer H of $\langle AB\rangle$ is a field extension of K, and we have

$$\dim_K\langle AB\rangle \geq \dim_K A + \dim_K B - \dim_K H. \tag{19}$$

Then H stabilizes $\langle ABC\rangle$, since $H\langle AB\rangle c = \langle AB\rangle c$ for all $c \in C$. Of course $\langle AB\rangle$ is a subspace of $\langle ABC\rangle$, since $1 \in C$. Assume $\langle ABC\rangle \neq \langle AB\rangle$. Since $H\langle ABC\rangle = \langle ABC\rangle$, Lemma 8.1 implies the existence of a nonempty finite subset $R \subset \langle ABC\rangle$ such that $R \cap \langle AB\rangle = \emptyset$ and

$$\langle ABC\rangle = \langle AB\rangle \oplus \bigoplus_{v\in R} Hv.$$

In particular, we have

$$\dim_K\langle ABC\rangle = \dim_K\langle AB\rangle + |R| \dim_K H.$$

Since $|R| > 0$, this gives

$$\dim_K\langle ABC\rangle \geq \dim_K\langle AB\rangle + \dim_K H.$$

Finally, by (19), we obtain the desired inequality

$$\dim_K\langle ABC\rangle \geq \dim_K A + \dim_K B.$$

■

Corollary 8.3 *Let $K \subset L$ be commutative fields such that every algebraic element in L is separable over K. Let A, B be nonzero finite-dimensional K-subspaces of L. Then either*

$$\langle ABB_*^{-1}B\rangle = \langle AB\rangle \quad \textit{or} \quad \dim_K\langle AB^2\rangle \geq \dim_K A + \dim_K B.$$

Proof. Assume $\langle ABB_*^{-1}B\rangle \neq \langle AB\rangle$. Then there exists $b_0 \in B$ such that $\langle ABb_0^{-1}B\rangle \neq \langle AB\rangle$. Thus $\langle ABb_0^{-1}Bb_0^{-1}\rangle \neq \langle ABb_0^{-1}\rangle$. We have $1 \in Bb_0^{-1}$. Thus, applying the above theorem to A and Bb_0^{-1}, we get

$$\dim_K\langle AB^2\rangle = \dim_K\langle ABb_0^{-1}Bb_0^{-1}\rangle \geq \dim_K A + \dim_K B.$$

■

9 Powers of subspaces

As in the preceding section, we assume that L is a commutative field extension of K in which every algebraic element is separable over K. If B is a nonzero finite-dimensional K-subspace of L, we shall consider the sequence of powers B, $\langle B^2\rangle, \langle B^3\rangle, \ldots$ and analyze the evolution of the nondecreasing sequence $\dim_K\langle B^i\rangle, i \geq 1$. Without loss of generality, replacing B by $b^{-1}B$ for some $b \in B \setminus \{0\}$, we may and will assume that B contains 1. Under this hypothesis, the sequence $\langle B^i\rangle$ turns into an ascending chain

$$B \subset \langle B^2\rangle \subset \langle B^3\rangle \subset \ldots.$$

This chain may eventually stabilize at $\langle B^n\rangle$ for some $n \geq 1$, for instance if L is finite-dimensional over K. We start by analyzing the least such exponent n, if any.

Proposition 9.1 *Let K be a commutative field and L a field extension of K containing K in its center. Let B be a finite-dimensional K-subspace of L containing 1. Let $n \geq 1$. The following are equivalent:*

(1) $\langle B^{n+1}\rangle = \langle B^n\rangle$;

(2) $\langle B^{2n}\rangle = \langle B^n\rangle$;

(3) $\langle B^n\rangle$ *is a field.*

Proof. First observe that, if U, V are any subsets of L, then

$$\langle UV\rangle = \langle\langle U\rangle\langle V\rangle\rangle.$$

Indeed, both K-subspaces are generated by the subset UV. In particular, we may and will freely use formulas such as $\langle B^m\rangle = \langle\langle B^i\rangle\langle B^{m-i}\rangle\rangle$ for integers $0 \leq i \leq m$.

Assume first $\langle B^{n+1}\rangle = \langle B^n\rangle$. Then we claim that $\langle B^{n+i}\rangle = \langle B^n\rangle$ for all $i \geq 1$. Indeed, proceeding by induction on i, we have

$$\langle B^{n+i}\rangle = \langle\langle B^{n+i-1}\rangle B\rangle = \langle B^{n+1}\rangle = \langle B^n\rangle.$$

For $i = n$, this gives $\langle B^{2n}\rangle = \langle B^n\rangle$. In turn, this equality is equivalent to $\langle\langle B^n\rangle\langle B^n\rangle\rangle = \langle B^n\rangle$. By Lemma 6.1, it follows that $\langle B^n\rangle$ is a field.

Conversely, if $\langle B^n \rangle$ is a field, then $\langle B^{2n} \rangle = \langle \langle B^n \rangle \langle B^n \rangle \rangle = \langle B^n \rangle$. As $\langle B^n \rangle \subset \langle B^{n+1} \rangle \subset \langle B^{2n} \rangle$, this implies that $\langle B^{n+1} \rangle = \langle B^n \rangle$. ■

In particular, the smallest integer $n \geq 1$, if any, such that $\langle B^n \rangle = \langle B^{n+1} \rangle$ coincides with the smallest integer $n \geq 1$, if any, such that $\langle B^n \rangle$ is a field.

Theorem 9.2 *Let K be a commutative field and L a commutative field extension of K. Suppose that every algebraic element in L is separable over K. Let B be a finite-dimensional K-vector space in L containing 1, and let $n \geq 1$. Then either*

$$\langle B^{n+1} \rangle = \langle B^n \rangle$$

or

$$\dim_K \langle B^{n+1} \rangle \geq \dim_K \langle B^{n-1} \rangle + \dim_K B.$$

Proof. Observe first that $\langle B^{n+1} \rangle = \langle B^n \rangle$ if and only if $\langle B^{n+1} \rangle = \langle B^n b \rangle$ for all $b \in B \setminus \{0\}$. Indeed, we have $\langle B^n \rangle \subset \langle B^n b \rangle \subset \langle B^{n+1} \rangle$, and $\langle B^{n+1} \rangle$ is the sum of all the subspaces $\langle B^n b \rangle$ where b runs over $B \setminus \{0\}$.

It follows that $\langle B^{n+1} \rangle = \langle B^n \rangle$ is equivalent to $\langle B^n b_1 \rangle = \langle B^n b_2 \rangle$ for all $b_1, b_2 \in B \setminus \{0\}$, which in turn is equivalent to $\langle B^n (B B_*^{-1}) \rangle = \langle B^n \rangle$.

Assume now $\langle B^n (B B_*^{-1}) \rangle \neq \langle B^n \rangle$. Since L is a commutative field, this is equivalent to $\langle B^n (B_*^{-1} B) \rangle \neq \langle B^n \rangle$. Applying Corollary 8.3 to B^{n-1} and B, this gives

$$\dim_K \langle B^{n+1} \rangle \geq \dim_K \langle B^{n-1} \rangle + \dim_K B,$$

as required. ■

Corollary 9.3 *Let K be a commutative field and L a finite separable commutative extension of K. Let B be a K-vector space in L containing 1. Then the smallest integer $n \geq 1$ such that $\langle B^n \rangle$ is a field satisfies*

$$n \leq 2 \dim_K L / \dim_K B.$$

Proof. By Proposition 9.1, we have $B \subsetneqq \langle B^2 \rangle \subsetneqq \cdots \subsetneqq \langle B^n \rangle$. It follows from Theorem 9.2 that

$$\dim_K \langle B^n \rangle \geq \begin{cases} \frac{(n+1)}{2} \dim_K B & \text{if } n \text{ is odd,} \\ \frac{n}{2} \dim_K B & \text{if } n \text{ is even.} \end{cases}$$

Since $\dim_K \langle B^n \rangle \leq \dim_K L$, this imposes the inequality

$$n \leq \begin{cases} 2\dim_K L/\dim_K B - 1 & \text{if } n \text{ is odd,} \\ 2\dim_K L/\dim_K B & \text{if } n \text{ is even.} \end{cases}$$

■

Remark. From the previous Corollary, we deduce

$$n \leq \left\lfloor \frac{2\dim_K L}{\dim_K B} \right\rfloor.$$

This upper bound is sharp. This can easily be seen, for example by choosing for B a supplementary space of K in L.

Acknowledgment. The authors thank Vincent Fleckinger, Joseph Oesterlé and Surya D. Ramana for stimulating discussions concerning Section 6 of this paper.

References

[1] X. D. Hou, K. H. Leung and Xiang. Q, *A generalization of an addition theorem of Kneser*, J. Number Theory **97** (2002), 1-9.

[2] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math **18** (1956), 247-254.

[3] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. **58** (1953), 459-484.

[4] M. Kneser, *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429-434.

[5] J. E. Olson, *On the sum of two sets in a group*, J. Number Theory **18** (1984), 110-120.