On the product of vector spaces in a commutative field extension

Shalom Eliahou, Michel Kervaire, Cédric Lecouvey

On the product of vector spaces in a commutative field extension

Shalom Eliahou, Michel Kervaire and Cédric Lecouvey

Abstract

Let $K \subset L$ be a commutative field extension. Given K-subspaces A, B of L, we consider the subspace $\langle AB \rangle$ spanned by the product set $AB = \{ab \mid a \in A, b \in B\}$. If $\dim_K A = r$ and $\dim_K B = s$, how small can the dimension of $\langle AB \rangle$ be? In this paper we give a complete answer to this question in characteristic 0, and more generally for separable extensions. The optimal lower bound on $\dim_K \langle AB \rangle$ turns out, in this case, to be provided by the numerical function

$$\kappa_{K,L}(r,s) = \min_h (\lceil r/h \rceil + \lceil s/h \rceil - 1)h,$$

where h runs over the set of K-dimensions of all finite-dimensional intermediate fields $K \subset H \subset L$. This bound is closely related to one appearing in additive number theory.

1 Introduction

Let $K \subset L$ be an extension of commutative fields. Let $A, B \subset L$ be non-zero K-subspaces of L. We denote by

$$\langle AB \rangle$$

the K-subspace of L generated by the product set

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

Of course, if A, B are finite-dimensional, then so is $\langle AB \rangle$ which satisfies the easy estimates

$$\max\{\dim_K A, \dim_K B\} \ \leq \ \dim_K \langle AB \rangle \ \leq \ (\dim_K A)(\dim_K B).$$

The above lower bound is sharp in the very special circumstance $A = B = H$ where H is an intermediate field extension $K \subset H \subset L$. But in general, if $\dim_K A, \dim_K B$ are specified in advance, how small can $\dim_K \langle AB \rangle$ be? In other words, given positive integers $r, s \leq \dim_K L$, we define

$$\mu_{K,L}(r,s) = \min\{\dim_K \langle AB \rangle\},$$

where the minimum is taken over all K-subspaces A, B of L satisfying

$$\dim_K A = r, \quad \dim_K B = s.$$

For example, one has $\mu_{K,L}(h,h) = h$ whenever $h = [H : K] = \dim_K H$ is the degree of a finite-dimensional intermediate field extension $K \subset H \subset L$.

Perhaps surprisingly, the combinatorial function $\mu_{K,L}(r,s)$ can be explicitly determined for arbitrary r, s under mild hypotheses, as we do here. Our answer is provided by the following numerical function. Define

$$\kappa_{K,L}(r,s) = \min_h (\lceil r/h \rceil + \lceil s/h \rceil - 1)h,$$

where $h = [H : K]$ runs over the set of K-dimensions of all finite-dimensional intermediate fields $K \subset H \subset L$.

For example, if $[L : K]$ is a prime number p, then the only admissible values for $h = [H : K]$ are 1 and p, whence $\kappa_{K,L}(r, s) = \min\{r + s - 1, p\}$. (See Example 5.2.) We shall prove the following result.

Theorem 1.1 *Let $K \subset L$ be a commutative field extension in which every algebraic element of L is separable over K. Then, for all positive integers $r, s \leq \dim_K L$, we have*

$$\mu_{K,L}(r, s) = \kappa_{K,L}(r, s).$$

There are close links between this result and additive number theory, as explained in Section 2. The proof of Theorem 1.1 is split between Sections 3 and 4. After some examples in Section 5, we look more closely, in Section 6, at the case of finite Galois extensions. In the last two sections, we discuss the separability hypothesis in Theorem 1.1.

2 Links with additive number theory

The question explored in this paper is analogous to a classical one in groups, namely that of minimizing the cardinality of product sets AB where A, B run over all subsets of cardinality r, s in a given group G. In multiplicative notation, this amounts to study the function

$$\mu_G(r, s) = \min\{|AB| \ : \ A, B \subset G, |A| = r, |B| = s\}.$$

While unknown in general, this function has recently been fully determined in the abelian case. The answer is expressed in terms of the numerical function $\kappa_G(r, s)$ defined as follows. For any group G, let $\mathcal{H}(G)$ be the set of orders of finite subgroups of G, and set

$$\kappa_G(r, s) = \min_{h \in \mathcal{H}(G)} (\lceil r/h \rceil + \lceil s/h \rceil - 1)h$$

for all positive integers $r, s \leq |G|$. Here is the result obtained in [1].

Theorem 2.1 *Let G be an arbitrary abelian group. Then, for all positive integers $r, s \geq 1$, we have $\mu_G(r, s) = \kappa_G(r, s)$.*

For instance, this contains the well-known Cauchy-Davenport theorem for cyclic groups G of prime order p, namely $\mu_G(r, s) = \min\{r + s - 1, p\}$ for all $1 \leq r, s \leq p$. See [3] for a survey of recent results on $\mu_G(r, s)$.

The function $\kappa_G(r, s)$ appears in various guises and contexts, for instance as the Hopf-Stiefel function $r \circ s$ in algebraic topology or in the theory of quadratic forms. See [2] for a survey on this ubiquitous function.

The reader will notice the close resemblance between Theorems 1.1 and 2.1. The methods of proof are also quite similar. In order to prove that the kappa-function is a lower bound, the key tools are a theorem of Kneser for abelian groups [8], and a linear version of it for separable extensions [6]. Regarding the optimality of the bound, the key tool is the *small sumsets property*, amounting to the inequality $\mu_G(r, s) \leq r + s - 1$ for abelian groups [1]. The analogous estimate for field extensions $K \subset L$, namely $\mu_{K,L}(r, s) \leq r + s - 1$, plays the same role and will be shown to hold in full generality.

In Section 6, we shall see that both versions of the kappa-function, namely κ_G for a group G and $\kappa_{K,L}$ for a field extension $K \subset L$, actually coincide for finite Galois extensions with abelian Galois group G.

For general background on commutative field extensions and on additive number theory, we refer to [7] and [9], respectively.

3 Proof that $\kappa_{K,L}$ is a lower bound

We now go back to the field extension setting. In order to prove inequality $\mu_{K,L}(r,s) \geq \kappa_{K,L}(r,s)$ of Theorem 1.1, we shall need the following linear version [6] of a famous theorem of Kneser [8] in additive number theory.

Theorem 3.1 (Hou, Leung and Xiang) *Let $K \subset L$ be a commutative 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. Let H be the stabilizer of $\langle AB \rangle$. Then*

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

The separability hypothesis of the above theorem is discussed in Section 8.

Proof of inequality $\mu_{K,L}(r,s) \geq \kappa_{K,L}(r,s)$ of Theorem 1.1. Let $A, B \subset L$ be K-subspaces of L with $\dim_K A = r$, $\dim_K B = s$. We must prove that $\dim_K \langle AB \rangle \geq \kappa_{K,L}(r,s)$. As in Theorem 3.1, let H be the stabilizer of the subspace $\langle AB \rangle$, i.e.

$$H = \{x \in L \mid x\langle AB \rangle \subset \langle AB \rangle\}.$$

Then of course, H is a subfield of L containing K, and we have

$$H\langle AB \rangle = \langle AB \rangle.$$

We shall apply Theorem 3.1 to the pair $\langle HA \rangle$, $\langle HB \rangle$ of K-subspaces of L. The first observation is that this pair has the same product as the pair A, B:

$$\langle \langle HA \rangle \langle HB \rangle \rangle = \langle HAB \rangle = \langle AB \rangle.$$

In particular, the stabilizer of the product is still H. By Theorem 3.1, we obtain

$$\dim_K \langle AB \rangle \geq \dim_K \langle HA \rangle + \dim_K \langle HB \rangle - \dim_K H.$$

Let $g = \dim_K H$. Factoring g in the above formula, we get

$$\dim_K \langle AB \rangle \geq \left(\frac{\dim_K \langle HA \rangle}{g} + \frac{\dim_K \langle HB \rangle}{g} - 1\right) g. \tag{1}$$

Now, $\langle HA \rangle$ is an H-subspace of L, and therefore $\dim_K \langle HA \rangle$ is a *multiple* of $\dim_K H = g$. Moreover, the integer $(\dim_K \langle HA \rangle)/g$ is greater than or equal to $(\dim_K A)/g = r/g$. It follows that

$$\frac{\dim_K \langle HA \rangle}{g} \geq \lceil \frac{r}{g} \rceil.$$

The same estimate holds with B, s replacing A, r, respectively. Plugging this information into inequality (1), we get

$$\dim_K\langle AB\rangle \geq (\lceil r/g\rceil + \lceil s/g\rceil - 1)g.$$

Finally, given that g is the dimension of an intermediate field $K \subset H \subset L$, we have

$$(\lceil r/g\rceil + \lceil s/g\rceil - 1)g \geq \kappa_{K,L}(r,s),$$

by definition of this κ-function. It follows that $\dim_K\langle AB\rangle \geq \kappa_{K,L}(r,s)$. We have now shown, as claimed, that

$$\mu_{K,L}(r,s) \geq \kappa_{K,L}(r,s)$$

for all positive integers $r, s \leq \dim_K L$. ■

4 Optimality

It remains to prove inequality $\mu_{K,L}(r,s) \leq \kappa_{K,L}(r,s)$ of Theorem 1.1. This is a construction problem. Given positive integers $r, s \leq \dim_K L$, we must exhibit a pair of K-subspaces $A, B \subset L$ with $\dim_K A = r$, $\dim_K B = s$ and $\dim_K\langle AB\rangle \leq \kappa_{K,L}(r,s)$. We start with a lemma on simple extensions.

Lemma 4.1 *Let $H \subset L$ be a commutative field extension, let $\alpha \in L$ and set $M = H(\alpha)$. Then, for all positive integers $r, s \leq \dim_H M$, we have*

$$\mu_{H,M}(r,s) \leq r + s - 1.$$

Proof. Assume first that α is transcendental over H. Given integers $r, s \geq 1$, let $A = \langle 1, \alpha, \ldots, \alpha^{r-1}\rangle$ be the H-subspace of M spanned by the first r powers of α, and similarly let $B = \langle 1, \alpha, \ldots, \alpha^{s-1}\rangle$. Then $\dim_H A = r$, $\dim_H B = s$ and $\dim_H\langle AB\rangle = \dim_H\langle 1, \alpha, \ldots, \alpha^{r+s-2}\rangle = r + s - 1$.

Assume now that α is algebraic over H, of degree $[M : H] = m$. In particular, the set $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is an H-basis of M. Given positive integers $r, s \leq m$, let $A = \langle 1, \alpha, \ldots, \alpha^{r-1}\rangle$ and $B = \langle 1, \alpha, \ldots, \alpha^{s-1}\rangle$ as above. Then $\dim_H A = r$, $\dim_H B = s$, and $\dim_H\langle AB\rangle \leq r + s - 1$ since $\langle AB\rangle$ is spanned by the set $\{\alpha^i\}_{0\leq i\leq r+s-2}$.

In either case, our explicit pair of subspaces A, B yields the desired estimate $\mu_{H,M}(r,s) \leq r + s - 1$. ■

As a side remark, note that the above formula remains valid if either $r = 0$ or $s = 0$, but not if both $r = s = 0$. Using the Primitive Element Theorem for separable extensions, here is a consequence that we shall need.

Proposition 4.2 *Let $H \subset L$ be a commutative field extension which is separable or contains a transcendental element. Then, for all positive integers $r, s \leq \dim_H L$, we have*

$$\mu_{H,L}(r,s) \leq r + s - 1.$$

Proof. If L contains a transcendental element α, we are done by the lemma above. (Indeed, with $M = H(\alpha)$ we have $\mu_{H,L}(r,s) \leq \mu_{H,M}(r,s) \leq r + s - 1$.) Assume now that L is algebraic and separable over H. Given positive integers $r, s \leq \dim_H L$, let $U \subset L$ be any linearly independent set of size $\max\{r, s\}$. Set $L_0 = H(U)$, the subfield of L generated by U over H. It follows from

the present assumptions on L, that L_0 is a finite and separable extension of H, with $[L_0 : H] = m \geq \max\{r, s\}$. By the Primitive Element Theorem, there exists an element $\alpha \in L_0$ such that $L_0 = H(\alpha)$. We now conclude with Lemma 4.1. ■

The above result is in fact valid without any separability hypothesis, as shown in Section 7 with a little longer argument. However, the present version is sufficient to help us conclude the proof of Theorem 1.1.

Proof of inequality $\mu_{K,L}(r, s) \leq \kappa_{K,L}(r, s)$. Let r, s be positive integers not exceeding $[L : K]$. Let $h_0 = [H : K]$ be the K-dimension of a finite-dimensional intermediate field extension $K \subset H \subset L$ for which $\kappa_{K,L}(r, s)$ attains its value, i.e. such that

$$\kappa_{K,L}(r, s) = (\lceil r/h_0 \rceil + \lceil s/h_0 \rceil - 1)h_0.$$

(Note that such an h_0 exists and cannot exceed $r + s - 1$ since, using $h = 1$ in the definition of $\kappa_{K,L}$, we have $\kappa_{K,L}(r, s) \leq r + s - 1$.) Set $r_0 = \lceil r/h_0 \rceil$, $s_0 = \lceil s/h_0 \rceil$. Of course $\lceil r/h_0 \rceil, \lceil s/h_0 \rceil \leq [L : K]/h_0 = [L : H]$. From the hypotheses on the extension L over K, it follows that L, as an extension over H, is either separable or else contains a transcendental element. By Proposition 4.2, we have $\mu_{H,L}(r_0, s_0) \leq r_0 + s_0 - 1$. Thus there exist H-subspaces $A_0, B_0 \subset L$ such that

$$\begin{aligned} \dim_H A_0 &= r_0, \\ \dim_H B_0 &= s_0, \\ \dim_H \langle A_0 B_0 \rangle &\leq r_0 + s_0 - 1. \end{aligned}$$

Now, viewed as K-subspaces of L, their dimensions are multiplied by h_0. Thus, we have

$$\begin{aligned} \dim_K A_0 &= r_0 h_0, \\ \dim_K B_0 &= s_0 h_0, \\ \dim_K \langle A_0 B_0 \rangle &\leq (r_0 + s_0 - 1)h_0 \;=\; \kappa_{K,L}(r, s). \end{aligned}$$

Therefore $\mu_{K,L}(r_0 h_0, s_0 h_0) \leq \kappa_{K,L}(r, s)$. Now $r \leq r_0 h_0$, $s \leq s_0 h_0$, and clearly the function $\mu_{K,L}(r, s)$ is nondecreasing in each variable. It follows that

$$\mu_{K,L}(r, s) \leq \mu_{K,L}(r_0 h_0, s_0 h_0) \leq \kappa_{K,L}(r, s),$$

as claimed. The proof of Theorem 1.1 is now complete. ■

5 Examples

We now give three examples illustrating Theorem 1.1.

Example 5.1 (Transcendental extensions) *Assume that L is a purely transcendental extension of K. In that case, the unique finite-dimensional intermediate extension $K \subset H \subset L$ is $H = K$ itself. It follows that $\kappa_{K,L}(r, s) = r + s - 1$ and thus, by Theorem 1.1, we have*

$$\mu_{K,L}(r, s) = r + s - 1$$

for all positive integers r, s. (See also Theorem 6.3 and the remark following it in [4].)

Example 5.2 (A linear version of the Cauchy-Davenport Theorem) *Let $K \subset L$ be a commutative field extension of prime degree $[L : K] = p$. Asssume that char(K) is distinct from p. Then, for all $1 \leq r, s \leq p$, we have*

$$\mu_{K,L}(r, s) = \min\{r + s - 1, p\}. \tag{2}$$

(Compare with the original Cauchy-Davenport Theorem in Section 2.) Indeed, by our assumption $\mathrm{char}(K) \neq p$, the extension is separable. Thus Theorem 1.1 applies and gives $\mu_{K,L}(r, s) = \kappa_{K,L}(r, s)$. Finally, since the only intermediate fields $K \subset H \subset L$ are $H = K$ and $H = L$, we have $\kappa_{K,L}(r, s) = \min\{r + s - 1, p\}$ by definition of this function.

Actually, formula (2) also holds if $\mathrm{char}(K) = p$, as we shall show in a future publication.

Example 5.3 (An extension of degree 16) *Consider the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[16]{2})$. This is a separable extension of degree 16, obviously containing intermediate extensions of degree 2, 4 and 8. It follows that, for all $1 \leq r, s \leq 16$, we have*

$$\mu_{\mathbb{Q},\mathbb{Q}(\sqrt[16]{2})}(r, s) = \kappa_{\mathbb{Q},\mathbb{Q}(\sqrt[16]{2})}(r, s) = \min_{h|16}(\lceil r/h \rceil + \lceil s/h \rceil - 1)h.$$

This is exactly the classical Hopf-Stiefel function $r \circ s$ [2]. We now tabulate this function in order to sense its quite complicated behavior. The value of $r \circ s$ is the coefficient in row r and column s of the matrix below:

$$\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
2 & 2 & 4 & 4 & 6 & 6 & 8 & 8 & 10 & 10 & 12 & 12 & 14 & 14 & 16 & 16 \\
3 & 4 & 4 & 4 & 7 & 8 & 8 & 8 & 11 & 12 & 12 & 12 & 15 & 16 & 16 & 16 \\
4 & 4 & 4 & 4 & 8 & 8 & 8 & 8 & 12 & 12 & 12 & 12 & 16 & 16 & 16 & 16 \\
5 & 6 & 7 & 8 & 8 & 8 & 8 & 8 & 13 & 14 & 15 & 16 & 16 & 16 & 16 & 16 \\
6 & 6 & 8 & 8 & 8 & 8 & 8 & 8 & 14 & 14 & 16 & 16 & 16 & 16 & 16 & 16 \\
7 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 15 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
10 & 10 & 12 & 12 & 14 & 14 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
11 & 12 & 12 & 12 & 15 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
12 & 12 & 12 & 12 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
13 & 14 & 15 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
14 & 14 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
15 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16
\end{pmatrix}$$

For example, one finds $11 \circ 4 = 12$ and $11 \circ 5 = 15$. The fact that the lower antidiagonal part of the matrix is constant and equal to 16 is part of the following more general phenomenon.

Remark 5.4 *If $[L : K] = n$, then $\kappa_{K,L}(r, s) = n$ whenever $r, s \leq n$ and $r + s \geq n + 1$.*

Indeed, denote $f_h(r, s) = (\lceil r/h \rceil + \lceil s/h \rceil - 1)h$. Then $\kappa_{K,L}(r, s) = \min_h f_h(r, s)$, where h runs over a certain set of divisors of n, namely the K-degrees of intermediate extensions. If $r + s \geq n + 1$, then $f_h(r, s) \geq n + 1 - h$. But since $f_h(r, s)$ is a multiple of h, it follows that $f_h(r, s) \geq n + h - h = n$. Finally, with $h = n$ we get $f_n(r, s) = n$, and the formula follows.

6 Finite Galois extensions

In this section we consider the case of a finite Galois extension $K \subset L$ with Galois group G, and attempt to compare the function κ_G from group theory to its linear version $\kappa_{K,L}$.

By basic Galois theory, there is a bijection between intermediate extensions $K \subset H \subset L$ and subgroups of $G = Gal(L/K)$, namely $H \mapsto Gal(L/H)$. The cardinality of the subgroup of G corresponding to H is given by the formula

$$|Gal(L/H)| = [L : H] = [L : K]/[H : K].$$

Recall that $\kappa_G(r, s)$ is defined, in the case at hand, by minimizing the expression

$$(\lceil r/h \rceil + \lceil s/h \rceil - 1)h$$

over all subgroup cardinalities $h = |Gal(L/H)| = [L : H]$. However, in the definition of $\kappa_{K,L}(r, s)$, the minimum is rather taken over the numbers $h = [H : K]$. Thus, the functions $\kappa_{K,L}(r, s)$ and $\kappa_G(r, s)$ cannot be directly compared in general, except in the particular case where all divisors of $|G|$ happen to be subgroup cardinalities; this occurs for instance if G is abelian or a p-group. This observation yields the following consequences of Theorem 1.1.

Corollary 6.1 *Let $K \subset L$ be a Galois extension with finite Galois group G of order n. Assume that every divisor d of n is a subgroup cardinality. Then, for all positive integers $r, s \leq n = [L : K]$, we have*

$$\mu_{K,L}(r, s) = \kappa_G(r, s) = \min_{d|n}(\lceil r/d \rceil + \lceil s/d \rceil - 1)d.$$

Assuming further that G is abelian, and using Theorem 2.1, we get an equality on the level of μ-functions.

Corollary 6.2 *Let $K \subset L$ be a Galois extension with finite abelian Galois group G of order n. Then, for all positive integers $r, s \leq n = [L : K]$, we have*

$$\mu_{K,L}(r, s) = \mu_G(r, s). \tag{3}$$

However, note that equality (3) does not hold in general if G is nonabelian, even if all divisors of $|G|$ are subgroup cardinalities. For instance, for the nonabelian group $G = \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3Z$ of order 21, it is known that $\mu_G(5, 9) = \kappa_G(5, 9) + 1 = 13$; this provides, by Corollary 6.1, a counterexample to equality (3).

7 The small products property

In this section we show that Proposition 4.2 is valid in an arbitrary commutative field extension $H \subset L$, not necessarily separable. Indeed, we shall prove that, for all positive integers $r, s \leq [L : H]$, there exist H-subspaces A, B of L with $\dim_H A = r$, $\dim_H B = s$ and $\dim_H \langle AB \rangle \leq r + s - 1$. We might call this the *small products property*, in analogy with the small sumsets property for groups.

Proposition 7.1 *Let $H \subset L$ be a commutative field extension. Then, for all positive integers $r, s \leq \dim_H L$, we have*

$$\mu_{H,L}(r, s) \leq r + s - 1.$$

Proof. As in the proof of Proposition 4.2, we are done if L contains a transcendental element over H. Assume now that L is algebraic over H. If $[L : H]$ is infinite, then L contains intermediary extensions $H \subset L' \subset L$ with $[L' : H]$ finite but arbitrarily large. (Indeed, take $L' = H(u_1, \ldots, u_n)$ for any finite choice of $u_1, \ldots, u_n \in L$.) Hence we may further assume that $[L : H]$ is finite. Let $H \subset M \subset L$ be an intermediate extension for which the statement of the proposition is true, namely satisfying

$$\mu_{H,M}(r_0, s_0) \leq r_0 + s_0 - 1 \tag{4}$$

for all $1 \leq r_0, s_0 \leq [M : H]$. Such extensions exist, for instance $M = H$. We may further assume that M is maximal for this small products property. If $M = L$ we are done. If not, let $\alpha \in L \setminus M$, say of degree d over M. For the record, the set $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an M-basis of $M(\alpha)$. We shall show that the statement of the proposition still holds for the extension $H \subset M(\alpha)$, a contradiction to the maximality of M.

Let $r, s \leq [M(\alpha) : H] = [M : H]d$. Performing a slightly modified euclidean division by $[M : H]$, we may write

$$\begin{aligned} r &= q_1[M : H] + r_0, \\ s &= q_2[M : H] + s_0, \end{aligned}$$

with remainders $1 \leq r_0, s_0 \leq [M : H]$ and quotients $q_1, q_2 \leq d - 1$.

Since $\mu_{H,M}(r_0, s_0) \leq r_0 + s_0 - 1$, we may choose H-subspaces $A_0, B_0 \subset M$ such that

$$\begin{aligned} \dim_H A_0 &= r_0, \\ \dim_H B_0 &= s_0, \\ \dim_H \langle A_0 B_0 \rangle &\leq r_0 + s_0 - 1. \end{aligned}$$

We may assume $q_1 + q_2 \geq 1$, for otherwise $r = r_0, s = s_0$ and we are done in this case by assumption on M. We now define

$$\begin{aligned} A &= M \cdot \{1, \alpha, \ldots, \alpha^{q_1 - 1}\} \oplus A_0 \cdot \alpha^{q_1}, \\ B &= M \cdot \{1, \alpha, \ldots, \alpha^{q_2 - 1}\} \oplus B_0 \cdot \alpha^{q_2}, \end{aligned}$$

provided $q_1, q_2 \geq 1$. If $q_1 = 0$ or $q_2 = 0$, we simply set $A = A_0$ or $B = B_0$, respectively. In all cases, viewing A, B as vector spaces over H, we have

$$\begin{aligned} \dim_H A &= q_1[M : H] + r_0 = r, \\ \dim_H B &= q_2[M : H] + s_0 = s. \end{aligned}$$

(Recall that $1, \alpha, \ldots, \alpha^{d-1}$ are linearly independent over M, that $q_1, q_2 \leq d - 1$ and that $A_0, B_0 \subset M$.) Now, taking the product of A and B, it is plain that we get

$$\langle AB \rangle \subset M \cdot \{1, \alpha, \ldots, \alpha^{q_1 + q_2 - 1}\} \oplus \langle A_0 B_0 \rangle \cdot \alpha^{q_1 + q_2}.$$

It follows that

$$\dim_H \langle AB \rangle \leq (q_1 + q_2)[M : H] + (r_0 + s_0 - 1) = r + s - 1,$$

and the proof of the proposition is complete. ∎

8 Two conjectures

In Theorems 1.1 and 3.1, the extension $K \subset L$ is assumed to have all its algebraic elements separable. Are these results still valid without this hypothesis? The answer for Theorem 3.1 is conjectured in [5] to be positive.

Conjecture 8.1 *(X.D.Hou) Let $K \subset L$ be a commutative field extension, and let $A, B \subset L$ be nonzero finite-dimensional K-subspaces of L. Let H be the stabilizer of $\langle AB \rangle$. Then*

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

It is shown in [5] that the statement of the conjecture holds for $\dim_K A \leq 5$.

It remains to decide whether the separability hypothesis in Theorem 1.1 can be removed. We conjecture that this is the case.

Conjecture 8.2 *Let $K \subset L$ be a commutative field extension. Then, for all positive integers $r, s \leq \dim_K L$, one should have*

$$\mu_{K,L}(r,s) = \kappa_{K,L}(r,s).$$

This conjecture in fact follows from Conjecture 8.1. Indeed, our proof of Theorem 1.1 relies on both Theorem 3.1 and Proposition 4.2. Removing the separability hypotheses in these two results yields Conjecture 8.1 and Proposition 7.1, respectively. With the latter statements, our proof of Theorem 1.1 becomes a derivation of Conjecture 8.2 from Conjecture 8.1. In particular, by the above-mentioned result in [5], Conjecture 8.2 holds at least for $r \leq 5$.

Of course, by Theorem 1.1, Conjecture 8.2 holds for all separable extensions, and in particular in characteristic 0.

Acknowledgment: During the preparation of this paper, the first author has partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

References

[1] S. Eliahou and M. Kervaire, *Minimal sumsets in infinite abelian groups*, Journal of Algebra **287** (2005), 449-457.

[2] S. Eliahou and M. Kervaire, *Old and new formulas for the Hopf-Stiefel and related functions*, Expositiones Mathematicae **23** (2005), 127-145.

[3] S. Eliahou and M. Kervaire, *Some extensions of the Cauchy-Davenport Theorem*, Electronic Notes in Discrete Mathematics **28** (2007), 557-564.

[4] S. Eliahou and C. Lecouvey, *On linear versions of some addition theorems*, Submitted (2007).

[5] X. D. Hou, *On a vector space analogue of Kneser's theorem*, Linear Algebra and its Applications **426** (2007), 214-227.

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

[7] S. Lang, Algebra (3rd edition), Springer Verlag, 2002.

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

[9] M. B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Graduate Text in Mathematics 165, Springer-Verlag, New York, 1996.

Authors' Addresses

Shalom Eliahou, 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
e-mail: eliahou@lmpa.univ-littoral.fr, lecouvey@lmpa.univ-littoral.fr

Michel Kervaire,
Département de Mathématiques
Université de Genève
2-4, rue du Lièvre, Case postale 64
CH-1211 Genève 24, Suisse
e-mail: Michel.Kervaire@math.unige.ch