

# REVISITING KNESER'S THEOREM FOR FIELD EXTENSIONS

CHRISTINE BACHOC, ORIOL SERRA, AND GILLES ZÉMOR

**ABSTRACT.** A Theorem of Hou, Leung and Xiang generalised Kneser's addition Theorem to field extensions. This theorem was known to be valid only in separable extensions, and it was a conjecture of Hou that it should be valid for all extensions. We give an alternative proof of the theorem that also holds in the non-separable case, thus solving Hou's conjecture. This result is a consequence of a strengthening of Hou et al.'s theorem that is inspired by an addition theorem of Balandraud and is obtained by combinatorial methods transposed and adapted to the extension field setting.

## 1. INTRODUCTION

Let  $G$  be an abelian group and let  $S$  and  $T$  be finite subsets of  $G$ . Denote by  $S + T$  the set defined by  $\{s + t : s \in S, t \in T\}$ . Sets  $S + T$  are often referred to as *sumsets*. Kneser's classical addition Theorem [12] states that sufficiently small sumsets are periodic, meaning they are stabilized by non-zero group elements.

**Theorem 1** (Kneser). *Let  $G$  be an abelian group and let  $S$  be non-empty, finite subsets of  $G$ . Then one of the following holds:*

- $|S + T| \geq |S| + |T| - 1$ ,
- *there exists a subgroup  $H \neq \{0\}$  of  $G$  such that  $S + T + H = S + T$ .*

Kneser's Theorem is more usually stated as  $|S + T| \geq |S| + |T| - |H(S + T)|$  where  $H(S + T) = \{x \in G : x + S + T = S + T\}$  denotes the stabilizer of  $S + T$ . However, this more precise inequality is easily derived from Theorem 1 which we chose to formulate in this way because it is better suited to the discussion of the strengthened versions that will follow. Kneser's Theorem is one of the founding theorems of additive combinatorics and has many applications to this field, and more generally to situations where statements on the structure of sumsets are useful, see [15, 19] for example.

---

*Mathematics Subject Classification:* 11P70.

Financial support for this research was provided by the "Investments for the future" Programme IdEx Bordeaux CPU (ANR-10-IDEX- 03-02) and the Spanish Ministerio de Economía y Competitividad under project MTM2014-54745-P

Consider now the context of field extensions. Let  $F$  be a field and let  $L$  be an extension field of  $F$ . If  $S$  and  $T$  are  $F$ -vector subspaces of  $L$ , we shall denote by  $ST$  the  $F$ -linear span of the set of products  $st$ ,  $s \in S$ ,  $t \in T$ .

The following Theorem was obtained by Hou, Leung and Xiang [9], as a transposition to field extensions of Kneser's classical addition Theorem.

**Theorem 2** (Hou, Leung and Xiang). *Let  $F$  be a field,  $L/F$  a field extension, and let  $S$  and  $T$  be  $F$ -subvectorspaces of  $L$  of finite dimension. Suppose that every algebraic element in  $L$  is separable over  $F$ . Then one of the following holds:*

- $\dim ST \geq \dim S + \dim T - 1$ ,
- *there exists a subfield  $K$ ,  $F \subsetneq K \subset L$ , such that  $STK = ST$ .*

The conclusion of the Theorem of Hou et al. given in [9] is that we have

$$\dim ST \geq \dim S + \dim T - \dim H(ST),$$

where  $H(ST) = \{x \in L : xST \subset ST\}$  denotes the stabilizer of  $ST$  in  $L$ . As is explained in [9], the above formulation is easily seen to be equivalent to the conclusion of Theorem 2. Hou et al.'s Theorem 2 can also be seen as a generalisation of the original additive Theorem of Kneser since the latter can be recovered from the former.

Theorem 2 was initially motivated by a problem on difference sets [9], but has since become part of a wider effort to transpose some classical theorems of additive combinatorics to a linear algebra or extension field setting. In particular Eliahou and Lecouvey [6] obtained linear analogues of some classical additive theorems including theorems of Olson [16] and Kemperman [11] in nonabelian groups. Lecouvey [14] pursued this direction by obtaining, among other extensions, linear versions of the Plünecké–Ruzsa [18] inequalities. The present authors recently derived a linear analogue of Vosper's Theorem in [1]. Somewhat more generally, additive combinatorics have had some spectacular successes by lifting purely additive problems into various algebras where the additional structure has provided the key to the original problems, e.g. [5, 10]. This provides in part additional motivation for linear extensions of classical addition theorems.

Going back to Hou et al.'s Theorem 2, a natural question is whether the separability assumption in Theorem 2 is actually necessary. Hou makes an attempt in [8] to work at Theorem 2 without the separability assumption, but only manages a partial result where the involved spaces are assumed to have small dimension. Hou goes on to conjecture [8] that Theorem 2 always holds, i.e., holds without the separability assumption. Recently, Beck and Lecouvey [3] extended Theorem 2 to algebras other than a field extension over  $F$ , but again, their approach breaks down when the algebra contains an infinity of subalgebras, so that the case of non-separable field extensions is not covered.

In the present work, we prove Hou's conjecture and remove the separability assumption in Theorem 2. We actually prove the stronger statement below.

**Theorem 3.** *Let  $L/F$  be a field extension, and let  $S \subset L$  be an  $F$ -subspace of  $L$  of finite positive dimension. Then*

- either for every finite dimensional subspace  $T$  of  $L$  we have

$$\dim ST \geq \dim S + \dim T - 1,$$

- or there exists a subfield  $K$  of  $L$ ,  $F \subsetneq K \subset L$ , such that for every finite-dimensional subspace  $T$  of  $L$  satisfying

$$\dim ST < \dim S + \dim T - 1,$$

we have  $STK = ST$ .

Besides the removal of the separability condition, the additional strength of Theorem 3 with respect to Theorem 2 lies in the fact that the subfield  $K$  that stabilises  $ST$  seems to depend on both spaces  $S$  and  $T$  in Theorem 2 but actually can be seen to depend only on one of the factors in Theorem 3. Theorem 3 is a transposition to the extension field setting of a theorem of Balandraud [2] which is a similarly stronger form of Kneser's Addition Theorem and can be stated as:

**Theorem 4.** *Let  $G$  be an abelian group, and let  $S \subset G$  be a finite subset of elements of  $G$ . Then*

- Either for every finite subset  $T$  of  $G$  we have

$$|S + T| \geq |S| + |T| - 1,$$

- or there exists a subgroup  $H \neq \{0\}$  of  $G$  such that, for every finite subset  $T$  of  $G$  satisfying

$$|S + T| < |S| + |T| - 1,$$

we have  $S + T + H = S + T$ .

Balandraud proved his theorem through an in-depth study of a phenomenon that he called saturation. For a given set  $S$ , a set  $T$  is saturated with respect to  $S$  if there does not exist a set  $T'$  strictly containing  $T$  such that the sums  $S + T$  and  $S + T'$  are equal. He showed that when  $T$  is a subset of smallest cardinality among all saturated subsets for which the quantity  $|S + T| - |T|$  is a given constant, then  $T$  must be a coset of some subgroup of  $G$ . Furthermore, the subgroups that appear in this way form a chain of nested subgroups, and the smallest non-trivial subgroup of this chain is the subgroup  $H$  of Theorem 4.

The techniques used by Balandraud are very combinatorial in nature and are inspired by Hamidoune's isoperimetric (or atomic) method in additive combinatorics [7, 17]. In the present paper we prove Theorem 3 by exporting Balandraud's approach to the extension field setting. This can also be seen as a follow-up to the linear isoperimetric method initiated in Section 3 of [1]. We note that this strategy deviates significantly from Hou et al.'s approach in [9] which relied on a linear variant of the additive  $e$ -transform and required crucially the separability of the field extensions.

We also note that Theorem 3 can be seen as a generalisation of Balandraud's Theorem 4 in groups, since the latter may be derived from the former by exactly the same Galois group argument as that of [9, Section 3].

The paper is organised as follows. Section 2 is devoted to setting up some basic tools and deriving the combinatorics of saturation. Section 3 introduces *kernels*, which are finite dimensional subspaces of minimum dimension among finite-dimensional subspaces  $T$  for which  $\dim ST - \dim T$  is a fixed integer less than  $\dim S - 1$ . A structural theory of kernels is derived, whose core features are collected in Theorem 15. Its proof is broken up into intermediate results through Propositions 20, 21 and 22. Finally, Section 4 derives the proof of Theorem 3 from the structure of kernels and concludes the paper.

## 2. PRELIMINARY DEFINITIONS AND PROPERTIES

We assume that  $L/F$  is a field extension and that  $S$  is a finite-dimensional  $F$ -subspace of  $L$  such that  $1 \in S$ . We suppose furthermore that  $F(S) = L$ , where  $F(S)$  denotes the subfield of  $L$  generated by  $S$ .

**2.1. Boundary operator and submodularity.** For every subspace  $X$  of  $L$  we define

$$\partial_S X = \dim XS/X$$

the increment of dimension of  $X$  when multiplied by  $S$ . We omit the subscript  $S$  in  $\partial_S$  whenever  $S$  is clear from the context. Note that we may have  $\partial X = \infty$  and that when  $X$  and  $S$  are finite-dimensional  $\partial X = \dim XS - \dim X$ . The essential property of the “boundary” operator  $\partial$  is the submodularity relation:

**Proposition 5.** *Let  $X, Y$  be subspaces of  $L$ . We have*

$$\partial(X + Y) + \partial(X \cap Y) \leq \partial X + \partial Y.$$

A short proof of Proposition 5 is given in [1] when  $L$  is finite-dimensional over  $F$ . In the general case, we invoke the following Lemma:

**Lemma 6.** *Let  $A, B, A'$  and  $B'$  be subspaces of some ambient vector space  $E$  such that  $A \subset A'$  and  $B \subset B'$ . There is an exact sequence of vector spaces*

$$0 \rightarrow (A' \cap B')/(A \cap B) \rightarrow A'/A \times B'/B \rightarrow (A' + B')/(A + B) \rightarrow 0.$$

*Proof.* We may identify the subspace  $A \cap B$  with the subspace of  $A \times B$  consisting of the elements  $(x, -x)$ ,  $x \in A \cap B$ . With the similar identification for  $A' \cap B'$ , we get the isomorphisms

$$(A \times B)/(A \cap B) \xrightarrow{\sim} A + B \quad \text{and} \quad (A' \times B')/(A' \cap B') \xrightarrow{\sim} A' + B' \quad (1)$$

and the following commutative diagram with the rows being exact and  $\gamma$  corresponding to the natural mapping of  $A + B$  into  $A' + B'$ .

$$\begin{array}{ccccccc} A \cap B & \longrightarrow & A \times B & \longrightarrow & (A \times B)/(A \cap B) & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & A' \cap B' & \longrightarrow & A' \times B' & \longrightarrow & (A' \times B')/(A' \cap B') \end{array}$$

The snake lemma (Lang, [13, Ch 3, Section 9]) therefore gives the exact sequence

$$0 \rightarrow \operatorname{coker} \alpha \rightarrow \operatorname{coker} \beta \rightarrow \operatorname{coker} \gamma \rightarrow 0,$$

which yields the result after identification of  $A' \times B'/A \times B$  with  $A'/A \times B'/B$  and the identifications (1).  $\square$

Lemma 6 immediately gives:

**Corollary 7.** *If  $A'/A$  and  $B'/B$  have finite dimension, then*

$$\dim (A' + B')/(A + B) = \dim A'/A + \dim B'/B - \dim (A' \cap B')/(A \cap B).$$

*Proof of Proposition 5.* If  $\partial X$  or  $\partial Y$  is  $\infty$ , there is nothing to prove, so we may set  $X' = XS$  and  $Y' = YS$  and suppose that  $X'/X$  and  $Y'/Y$  are finite-dimensional. We have  $(X+Y)S \subset X' + Y'$  and  $(X \cap Y)S \subset X' \cap Y'$ , whence

$$\partial(X + Y) + \partial(X \cap Y) \leq \dim (X' + Y')/(X + Y) + \dim (X' \cap Y')/(X \cap Y),$$

and the conclusion follows from Corollary 7.

**2.2. Duality.** Recall that every non-zero linear form  $\sigma : L \rightarrow F$  induces a nondegenerate symmetric bilinear (Frobenius) form defined as  $(x|y)_\sigma = \sigma(xy)$ , with the property:

$$(xy|z)_\sigma = (x|yz)_\sigma \text{ for all } x, y, z \in L. \quad (2)$$

Fix such a bilinear form  $(\cdot|\cdot)$ . For a subspace  $X$ , we set

$$X^\perp = \{y \in L : \forall x \in X, (x|y) = 0\}.$$

We call the *dual subspace* of the subspace  $X$  the subspace

$$X^* = (XS)^\perp.$$

We will use the notation  $X^{**} = (X^*)^*$  and  $X^{***} = (X^{**})^* = (X^*)^{**}$ .

We shall require the following lemma which is a straightforward consequence of Bourbaki [4, Ch. 9, §1, n. 6, Proposition 4]:

**Lemma 8.** *If  $A$  and  $B$  are subspaces such that the quotient  $A/(B^\perp \cap A)$  is finite dimensional, then  $\dim A/(B^\perp \cap A) = \dim B/(A^\perp \cap B)$ .*

The following elementary properties hold for subspaces and their duals:

**Lemma 9.** *For every  $F$ -subspace  $X$  of  $L$ , we have*

- (i)  $X \subset X^{**}$ .
- (ii)  $X^* = X^{***}$
- (iii)  $\partial X^* \leq \partial X$ .

*Proof.*

- (i) Let  $x \in X$  and let  $x^* \in X^*$  and  $s \in S$ . By definition of  $X^*$  we have  $(xs | x^*) = 0$ , so that  $(x | x^*s) = 0$ . Therefore  $x \in (X^*S)^\perp = X^{**}$ .
- (ii) Applying (i), we have  $X^* \subset (X^*)^{**}$ . Also, if  $Y \subset Z$ , then  $Z^* \subset Y^*$ , which yields  $(X^{**})^* \subset X^*$ .
- (iii) If  $\partial X = \infty$  there is nothing to prove, so assume  $\partial X < \infty$ . From (i) and  $X \subset XS$ , we have  $X \subset (X^{**} \cap XS)$ . Hence

$$\dim XS / (X^{**} \cap XS) \leq \dim XS / X < \infty.$$

Applying Lemma 8, we therefore have

$$\begin{aligned} \partial X^* &= \dim X^*S / X^* = \dim X^*S / (XS)^\perp = \dim XS / ((X^*S)^\perp \cap XS) \\ &= \dim XS / (X^{**} \cap XS) \leq \dim XS / X = \partial X. \end{aligned}$$

□

One would expect the stronger properties  $X^{**} = X$  and  $\partial X^* = \partial X$  to hold. Unfortunately this is not true for all subspaces, only for those who are *saturated*, a notion that we introduce below.

**2.3. Saturated spaces.** For a subspace  $X$  let us define the subspace  $\tilde{X}$  to be the set of all  $x \in L$  such that

$$xS \subset XS.$$

Clearly we have  $X \subset \tilde{X}$ ,  $\tilde{X}S = XS$ , and  $\partial \tilde{X} \leq \partial X$ . We remark also that  $\tilde{X} \subset \tilde{X}S = XS$  implies that whenever  $X$  is finite-dimensional, so is  $\tilde{X}$ .

A subspace  $X$  is said to be *saturated* if

$$\tilde{X} = X.$$

**Lemma 10.** *For every  $F$ -subspace  $X$  of  $L$ , the following hold:*

- (i)  $X^*$  is saturated.
- (ii) If  $X$  is finite-dimensional then  $X^{**} = \tilde{X}$ . In particular a finite-dimensional subspace  $X$  is saturated if and only if  $X = X^{**}$ .

*Proof.*

- (i) Let  $y \in L$  be such that  $yS \subset X^*S$ , and let us prove that  $y \in X^* = (XS)^\perp$ . Since  $ys \in X^*S$ , we have  $ys = \sum x_i^* s_i$  where  $x_i^* \in X^*$  and  $s_i \in S$ . Therefore, for any  $x \in X$ ,  $s \in S$ , we have

$$(y | xs) = (ys | x) = \sum_i (x_i^* s_i | x) = \sum_i (x_i^* | s_i x) = 0,$$

which means that  $y \in X^*$ .

- (ii) We recall that, for a finite-dimensional subspace  $A$ , we have  $(A^\perp)^\perp = A$  (Bourbaki, [4, Ch. 9, §1, n. 6, cor. 1]). The assertion follows from:

$$\begin{aligned}
 y \in X^{**} &\Leftrightarrow y \in (X^*S)^\perp \\
 &\Leftrightarrow \forall x^* \in X^*, \forall s \in S, (y | x^*s) = 0 \\
 &\Leftrightarrow \forall x^* \in X^*, \forall s \in S, (ys | x^*) = 0 \\
 &\Leftrightarrow yS \subset ((XS)^\perp)^\perp = XS \\
 &\Leftrightarrow y \in \tilde{X}.
 \end{aligned}$$

□

We denote by  $\mathcal{S}$  the family of saturated finite-dimensional subspaces  $X$  of  $L$  together with their duals  $X^*$ . We make the remark that, applying Lemma 8 with  $A = XS$  and  $B = L$ , the dual of a finite dimensional space has finite co-dimension (where the co-dimension of a space  $A$  is defined as  $\dim L/A$ ). In particular, elements of  $\mathcal{S}$  have either finite dimension or finite co-dimension.

The next lemma summarizes the properties of the elements of  $\mathcal{S}$  that we will need in the proof of Theorem 3.

**Lemma 11.** *For every  $X \in \mathcal{S}$ ,  $Y \in \mathcal{S}$ ,*

- (i)  $X$  is saturated and  $X^* \in \mathcal{S}$ .
- (ii)  $X^{**} = X$ .
- (iii)  $\partial X = \partial X^*$ .
- (iv)  $X \cap Y \in \mathcal{S}$ .
- (v)  $(X + Y)^{**} \in \mathcal{S}$ .

*Proof.*

- (i) (ii)  $X$  is saturated by Lemma 10(i). If  $X \in \mathcal{S}$  has finite dimension,  $X^*$  belongs to  $\mathcal{S}$  by definition, and  $X^{**} = X$  by Lemma 10(ii). Otherwise,  $X = X_1^*$  where  $X_1$  is saturated and of finite dimension, and  $X^* = X_1^{**} = X_1$  by Lemma 10(ii), so  $X^*$  belongs to  $\mathcal{S}$  and  $X^{**} = X_1^* = X$ .
- (iii) From Lemma 9(iii), we have  $\partial X^* \leq \partial X$ . Additionally, applying this inequality to  $X^*$  and combining with  $X^{**} = X$  leads to  $\partial X^* = \partial X$ .
- (iv) We have

$$X^* \cap Y^* = (XS)^\perp \cap (YS)^\perp = (XS + YS)^\perp = ((X + Y)S)^\perp = (X + Y)^*.$$

In particular, if  $X$  and  $Y$  belong to  $\mathcal{S}$ ,  $X \cap Y = X^{**} \cap Y^{**} = (X^* + Y^*)^*$  so, by Lemma 10(i),  $X \cap Y$  is saturated. If, moreover,  $X$  or  $Y$  is of finite dimension, we can conclude that  $X \cap Y \in \mathcal{S}$ . Otherwise,  $X = X_1^*$  and  $Y = Y_1^*$ , where  $X_1$  and  $Y_1$  are both of finite dimension, and  $X \cap Y = (X_1 + Y_1)^*$ . We remark that  $(X_1 + Y_1)^* = (X_1 + Y_1)^{***} = \widetilde{(X_1 + Y_1)^*}$ , applying Lemma 9(ii) and Lemma 10(ii), so  $X \cap Y \in \mathcal{S}$ .

- (v) If the dimensions of  $X$  and  $Y$  are finite, then, by Lemma 10(ii),  $(X + Y)^{**} = \widetilde{X + Y}$  belongs to  $\mathcal{S}$ . Otherwise, without loss of generality we may assume that  $X = X_1^*$  where  $X_1$  is saturated and of finite dimension. Let  $Z := (X + Y)^*$ . By Lemma 10(i),  $Z$  is saturated, and by Lemma 10(ii),  $Z \subset X^* = X_1^{**} = X_1$ , so  $Z$  is of finite dimension and we can conclude that  $Z^* = (X + Y)^{**}$  belongs to  $\mathcal{S}$ .

□

In the proof of Theorem 3, we will apply many times the submodularity inequality of Proposition 5 to certain subspaces  $X$  and  $Y$  belonging to  $\mathcal{S}$ . We will have  $X \cap Y \in \mathcal{S}$  (Lemma 11 (iv)), but we will have to deal with the issue that in general  $X + Y \notin \mathcal{S}$ . Lemma 11 (v) will allow us to replace  $X + Y$  by the larger  $(X + Y)^{**}$  since  $\partial(X + Y)^{**} \leq \partial(X + Y)$ . The following Lemma will be used several times in order to ensure that  $(X + Y)^{**} \neq L$  holds and that we do not have  $\partial(X + Y)^{**} = 0$ .

**Lemma 12.** *Let  $X$  and  $Y$  be subspaces of  $L$  such that  $\dim X < \infty$ ,  $\dim XS \leq \dim X + \dim S - 1$ ,  $\dim(X \cap Y) \geq 1$  and  $\dim X \leq \dim Y^*$ . Then*

$$(X + Y)^{**} \neq L.$$

*Proof.* We will prove that  $(X + Y)^* = (X + Y)^{***} \neq L^* = \{0\}$ . Since  $Y \subset (X + Y)$ , we have  $(X + Y)^* \subset Y^*$ . We will show that  $\dim Y^*/(X + Y)^*$  is finite and less than  $\dim(Y^*)$ , which will imply  $(X + Y)^* \neq \{0\}$ . Note that

$$YS \subset ((YS)^\perp)^\perp \cap (X + Y)S \subset (X + Y)S \subset XS + YS.$$

Therefore

$$\dim(X + Y)S / \left( ((YS)^\perp)^\perp \cap (X + Y)S \right) \leq \dim(XS + YS) / YS.$$

The right-hand side is finite, whence also the left-hand side, which, by Lemma 8, equals  $\dim Y^*/(X + Y)^*$ . We therefore have

$$\begin{aligned} \dim Y^*/(X + Y)^* &\leq \dim(XS + YS) / YS = \dim XS / (XS \cap YS) \\ &= \dim XS - \dim(XS \cap YS). \end{aligned}$$

From the hypothesis we have  $\dim XS \leq \dim X + \dim S - 1$  and from  $\dim(X \cap Y) \geq 1$  we have  $\dim(XS \cap YS) \geq \dim S$ . Hence

$$\dim Y^*/(X + Y)^* \leq \dim X + \dim S - 1 - \dim S = \dim X - 1 < \dim Y^*.$$

□

When trying to prove that a saturated subspace  $X$  has a non-trivial stabilizer, it will be useful to consider its dual subspace instead. The last Lemma of this section states that an element stabilizes a saturated subspace if and only if it stabilizes its dual subspace.

**Lemma 13.** *If  $X \in \mathcal{S}$  and  $k \in L$ , then  $kX \subset X$  if and only if  $kX^* \subset X^*$ .*



*Proof.* For  $x^* \in X^*$ ,  $x \in X$  and  $s \in S$ , we have

$$(kx^* | xs) = (x^* | kxs)$$

from which we get that if  $kX \subset X$  then  $(kx^* | xs) = 0$  for every  $x, x^*, s$ , whence  $kx^*$  is in  $X^*$ . Therefore  $kX^* \subset X^*$ .

if  $kX^* \subset X^*$  then we have just proved that  $kX^{**} \subset X^{**}$ , and Lemma 11 (ii) gives the desired conclusion.  $\square$

We remark that if  $X$  is finite dimensional and if  $kX \subset X$  for some non-zero  $k$ , then  $k$  can only be of finite degree over  $F$ , and we have  $k^{-1}X \subset X$ , (and therefore  $X = kX$ ). The stabilizer  $H(X) = \{k \in L, kX \subset X\}$  is a field in this case. Lemma 13 implies in particular that stabilizers of spaces of  $\mathcal{S}$  are subfields of  $L$ . Summarizing:

**Corollary 14.** *If  $X \in \mathcal{S}$ , then the stabilizer  $H(X)$  is a subfield satisfying  $H(X) = H(X^*)$ .*

### 3. STRUCTURE OF CELLS AND KERNELS OF A SUBSPACE

We assume, like in the previous section, that  $S$  is a finite dimensional  $F$ -subspace of  $L$  containing 1, and that  $L = F(S)$ . We will moreover assume that there does not exist a field  $K$ ,  $F \subsetneq K \subset L$ , such that  $KS = S$  (in other words  $H(S) = F$ ). Note that when such a  $K$  exists, the conclusion of Theorem 3 holds trivially. With the objective of working towards a proof of Theorem 3, we will also assume that there exists a non-zero finite dimensional subspace  $T \subset L$  such that  $ST \neq L$  and

$$\dim ST < \dim S + \dim T - 1.$$

Equivalently,  $\partial T < \dim S - 1$ .

Let

$$\Lambda = \{\partial(X) : X \in \mathcal{S}\}.$$

We denote the elements of  $\Lambda$  by

$$\Lambda = \{0 = \lambda_0 < \lambda_1 < \lambda_2 < \dots\}$$

and by

$$\mathcal{S}_i = \{X \in \mathcal{S} : \partial X = \lambda_i\}.$$

Spaces belonging to a set  $\mathcal{S}_i$  will be called *i-cells*. By Lemma 11 (i) (iii), the dual of an *i-cell* is an *i-cell*. An *i-cell* of smallest dimension will be said to be an *i-kernel*. We note that *i-kernels* are always of finite dimension, because the dual of an infinite-dimensional *i-cell* is an *i-cell* and must have finite dimension.

Suppose  $X$  is finite-dimensional and  $SX = X$ . Then either  $X = \{0\}$  or  $S$  must be a field, so that  $S = F(S) = L$ . From this we get that  $\mathcal{S}_0 = \{\{0\}, L\}$ . From our assumption on the existence of  $T$ , we get  $\lambda_1 < \dim S - 1$ . Let  $n$  be the largest integer such that  $\lambda_n < \dim S$ . We note that we have  $\lambda_n = \dim S - 1$  and that  $F$  is an  $n$ -kernel since  $\partial F = \dim S - 1$  and  $F$  is saturated, otherwise  $\tilde{F}$  would contradict our assumption on the non-existence of a field  $K \neq F$  such that  $KS = S$ .

If  $N$  is an  $i$ -kernel, then clearly so is  $xN$  for any non-zero  $x \in L$ . Therefore, when an  $i$ -kernel exists, there exists in particular an  $i$ -kernel containing  $F$ . Let  $F_1, F_2, \dots, F_n$  be  $1, 2, \dots, n$ -kernels containing  $F$ , which implies  $F_n = F$  by the remark just above.

Our core result is the following theorem.

**Theorem 15.** *We have*

$$F_1 \supset F_2 \supset \dots \supset F_n.$$

*Furthermore the  $F_i$  are all subfields of  $L$ , and every space  $X \in \mathcal{S}_i$  is stabilized by  $F_i$ .*

Note that this last statement implies in particular that the  $i$ -kernel containing  $F$  is unique.

We shall prove Theorem 15 in several steps.

First we prove the result for  $F_1$ . This simple case illustrates the general methodology that consists in intersecting the cell under study  $X$  with some other cell  $Y$ , and applying the submodularity relation of Proposition 5. The goal is to prove that the intersection  $X \cap Y$  is either  $X$  or  $Y$  by arguing that one of the two-cells is a kernel, and that it has minimum dimension among cells with a given boundary. For this one needs to bound from above the boundary of the intersection  $X \cap Y$ , which is achieved through Proposition 5 and a lower bound on the boundary of the sum  $X + Y$ . Most of the technicalities go into deriving these lower bounds.

**Proposition 16.**  *$F_1$  is a subfield of  $L$  and any 1-cell  $X$  satisfies  $XF_1 = X$ .*

*Proof.* Let  $X$  be a 1-cell and let  $x$  be a non-zero vector of  $X$ , so that  $X$  has a non-zero intersection with  $xF_1$ . By submodularity we have

$$\partial(xF_1 + X)^{**} + \partial(xF_1 \cap X) \leq \partial(xF_1 + X) + \partial(xF_1 \cap X) \leq 2\lambda_1.$$

By Lemma 11 (iv) we have  $xF_1 \cap X \in \mathcal{S}$ . Since  $xF_1 \cap X$  is non-zero and not equal to  $L$  (because  $F_1 \neq L$ ),  $xF_1 \cap X \in \mathcal{S}_k$  for some  $k \geq 1$ . Since  $xF_1$  is a 1-kernel, and since  $X^*$  is also a 1-cell, we have  $\dim xF_1 \leq \dim X^*$  and since kernels are finite-dimensional, Lemma 12 implies  $(xF_1 + X)^{**} \in \mathcal{S}_\ell$  for some  $\ell \geq 1$ . It follows that  $k = \ell = 1$ . Therefore,  $xF_1 \cap X$  is a 1-cell and, by the minimality of the dimension of 1-kernels, we have  $xF_1 \subset X$ . Since this holds for an arbitrary  $x \in X$ , we have proved  $XF_1 = X$ . Applying this to  $X = F_1$  we obtain that  $F_1$  is a subfield of  $L$ .  $\square$

Let  $J$  be the set of positive integers  $j \in [1, \dots, n]$  satisfying the conditions

- $F_1 \supset \dots \supset F_{j-1} \supset F_j$
- $F_j$  is a subfield of  $L$
- any  $j$ -cell is stabilized by  $F_j$ .

Proposition 16 tells us that  $1 \in J$ , so that  $J \neq \emptyset$ . The proof of Theorem 15 will be complete if we can show that  $J$  equals the whole interval  $[1, n]$ . We therefore assume by contradiction that  $\overline{J} = [1, n] \setminus J \neq \emptyset$  and define  $i$  to be the smallest integer in  $\overline{J}$ . We then proceed to show that the integer  $i$  also satisfies the above three conditions, contradicting  $i \notin J$ . Specifically

we shall prove that  $F_i \subset F_{i-1}$  (Proposition 20), that  $F_i$  is also a subfield (Proposition 21) and that  $F_i$  stabilizes every  $i$ -cell (Proposition 22).

**Lemma 17.** *No  $i$ -cell  $X$  is stabilized by  $F_{i-1}$ .*

*Proof.* Suppose  $F_{i-1}X = X$ . Then  $X$  and  $SX$  are  $F_{i-1}$ -vector spaces and  $\lambda_i = \dim XS/X$  is a multiple of  $\dim F_{i-1}$ . The quantity  $\lambda_{i-1} = \dim F_{i-1}S - \dim F_{i-1}$  is also a multiple of  $\dim F_{i-1}$ , and since  $\lambda_i > \lambda_{i-1}$ ,

$$\lambda_i \geq \lambda_{i-1} + \dim F_{i-1} = \dim F_{i-1}S \geq \dim S,$$

contradicting  $\lambda_i < \dim S$ .  $\square$

**Lemma 18.** *Let  $1 \leq j \leq i-1$ , and suppose  $\dim F_i \leq \dim F_j$ . Then, for any  $x \in F_i$  we have  $(xF_j + F_i)^{**} \neq F_{j-1}$ , where we adopt the convention  $F_0 = L$ . In particular if  $\dim F_i \leq \dim F_1$ , then  $(xF_1 + F_i)^{**} \neq L$ .*

*Proof.* Let  $x \in F_i$ . We have

$$\begin{aligned} \dim(xF_j + F_i)S &\leq \dim(xF_jS + F_iS) \\ &\leq \dim xF_jS + \dim F_iS - \dim(xF_jS \cap F_iS) \\ &\leq \dim F_jS + \dim F_iS - \dim S \end{aligned}$$

since  $xS \subset (xF_jS \cap F_iS)$ . From this we get

$$\dim(xF_j + F_i)S < \dim F_jS + \dim F_i,$$

since  $\dim F_iS \leq \dim F_i + \dim S - 1$ . But  $F_j \subsetneq F_{j-1}$  implies that  $F_jS \subset F_{j-1}S$ , whence  $F_jS \subsetneq F_{j-1}S$ , since  $F_jS = F_{j-1}S$  would contradict  $F_j$  being saturated. Now since  $F_jS$  and  $F_{j-1}S$  are both stabilized by  $F_j$  we obtain

$$\dim F_jS \leq \dim F_{j-1}S - \dim F_j,$$

whence

$$\dim(xF_j + F_i)S < \dim F_{j-1}S - \dim F_j + \dim F_i \leq \dim F_{j-1}S, \quad (3)$$

by the hypothesis  $\dim F_i \leq \dim F_j$ . To conclude, recall from Lemma 10 (ii) that  $(xF_j + F_i)^{**}S = (xF_j + F_i)S$ , so that  $(xF_j + F_i)^{**} = F_{j-1}$  would contradict (3).  $\square$

**Lemma 19.**  $F_i \subset F_1$ .

*Proof.* By Lemma 17, there exists  $x \in F_i$  such that  $F_{i-1}x \not\subset F_i$ . We have

$$\partial(xF_1 + F_i) + \partial(xF_1 \cap F_i) \leq \lambda_1 + \lambda_i. \quad (4)$$

Suppose that  $\dim F_i \leq \dim F_1$ . Then Lemma 18 implies that  $\widetilde{xF_1 + F_i} = (xF_1 + F_i)^{**} \neq L$ , so that  $\partial(xF_1 + F_i) \geq \partial(\widetilde{xF_1 + F_i}) \geq \lambda_1$ . If  $\dim F_i \leq \dim F_1$  does not hold, then  $\dim xF_1 < \dim F_i \leq \dim F_i^*$ , and Lemma 12 implies  $\partial(xF_1 + F_i) \geq \partial(\widetilde{xF_1 + F_i}) \geq \lambda_1$  again. In both cases, we obtain from (4) that  $\partial(xF_1 \cap F_i) \leq \lambda_i$ . Now  $xF_1 \cap F_i$  is saturated and contains  $x$ , but not  $F_{i-1}x$  and not  $F_jx$  either for  $j \leq i-1$  since  $F_j \supset F_{i-1}$ . Since we know that  $j$ -cells are stabilized by  $F_j$  for all  $j \leq i-1$ , we obtain that  $xF_1 \cap F_i$  cannot be a  $j$ -cell for all  $j \leq i-1$ . This implies in particular that  $\partial(xF_1 \cap F_i) \neq \lambda_j$  for all  $j \leq i-1$ . Hence,

$\partial(xF_1 \cap F_i) = \lambda_i$  which implies that  $F_i \subset xF_1$  by minimality of  $F_i$  in  $\mathcal{S}_i$ . Since  $1 \in F_i$  we must have  $1 \in xF_1$  which implies  $xF_1 = F_1$ .  $\square$

**Proposition 20.** *For every  $j < i$  we have  $F_i \subset F_j$ .*

*Proof.* We prove this by induction on  $j$ . Lemma 19 gives the result for  $j = 1$ , so suppose we already have  $F_i \subset F_{j-1}$  and let us prove  $F_i \subset F_j$ . Suppose first that  $\dim F_i > \dim F_j$ . Let  $x \in F_i^*$  and consider  $Z := (xF_j + F_i^*)^{**}$ , which belongs to  $\mathcal{S}$  by Lemma 11 (v). We have, by Proposition 5 and Lemma 9,

$$\partial Z + \partial(xF_j \cap F_i^*) \leq \partial(xF_j + F_i^*) + \partial(xF_j \cap F_i^*) \leq \lambda_j + \lambda_i.$$

By Lemma 12, since we assume that  $\dim F_i^{**} = \dim F_i \geq \dim F_j$ , we have  $Z \neq L$ , and by the induction hypothesis  $F_i \subsetneq F_{j-1}$ , we have  $F_i^* \supsetneq F_{j-1}^*$ , so that  $Z \supsetneq F_{j-1}^*$  and  $Z^* \subsetneq F_{j-1}$ . Therefore  $Z^*$  is not a  $(j-1)$ -cell by the minimality of  $\dim F_{j-1}$  in  $\mathcal{S}_{j-1}$ , from which it is not a  $k$ -cell for  $k < j$  in view of  $F_1 \supset \dots \supset F_{i-1}$ . Since the dual of a  $k$ -cell is again a  $k$ -cell, this implies that  $Z$  is also not a  $k$ -cell for all  $k < j$ . Therefore  $\partial Z \geq \lambda_j$ , which implies  $\partial(xF_j \cap F_i^*) \leq \lambda_i$ . Now, by the hypothesis  $\dim F_i > \dim F_j$ , we have that  $\dim(xF_j \cap F_i^*) < \dim F_i$  and  $xF_j \cap F_i^*$  cannot be an  $i$ -cell. Therefore it is in  $\mathcal{S}_k$  for some  $k < i$ , which, by definition of  $i$ , implies that it is stabilized by  $F_k$  and hence by  $F_{i-1}$ . By applying this to  $xF_j$  for every  $x \in F_i^*$ , we get that the whole of  $F_i^*$  is stabilized by  $F_{i-1}$ : but this contradicts Lemma 17. Hence

$$\dim F_i \leq \dim F_j. \quad (5)$$

Next, consider  $x \in F_i$ . Suppose that for every  $x \in F_i$ ,  $x \neq 0$ ,  $xF_j \cap F_i$  is in  $\mathcal{S}_k$  for some  $k < i$ . Then every  $xF_j \cap F_i$  is stabilized by  $F_{i-1}$  and  $F_{i-1}F_i = F_i$  which contradicts Lemma 17. Therefore there exists  $x \in F_i$  such that  $xF_j \cap F_i$  is not in  $\mathcal{S}_k$  for every  $k < i$ . This choice of  $x$  ensures that  $\partial(xF_j \cap F_i) \geq \lambda_i$ . If we can show that  $\partial(xF_j \cap F_i) = \lambda_i$ , we will conclude that  $F_i \subset xF_j$  by the minimality of the  $i$ -kernel  $F_i$ , and since  $1 \in F_i$  we will have  $1 \in xF_j$  and  $xF_j = F_j$ , so that  $F_i \subset F_j$  and we will be done. Consider now

$$\partial(xF_j + F_i) + \partial(xF_j \cap F_i) \leq \lambda_j + \lambda_i.$$

This inequality will yield  $\partial(xF_j \cap F_i) \leq \lambda_i$  and the desired result if we can show that

$$\partial(xF_j + F_i) \geq \lambda_j. \quad (6)$$

Inequality (6) will in turn follow if we show that  $(xF_j + F_i)^{**}$  is not a  $k$ -cell for  $k < j$ . We have  $xF_j \subset xF_{j-1}$  and, by the induction hypothesis on  $j$ , we have  $F_i \subset F_{j-1}$ , whence  $xF_{j-1} = F_{j-1}$  since  $x \in F_i$ . Therefore  $xF_j + F_i \subset F_{j-1}$ . From this we derive  $(xF_j + F_i)^{**} \subset F_{j-1}^{**}$  and  $(xF_j + F_i)^{**} \subset F_{j-1}$  by Lemma 11 (ii). Since  $F_{j-1} \subsetneq F_k$  for all  $k < j-1$ , we have, by minimality of  $F_k$  in  $\mathcal{S}_k$ , that  $(xF_j + F_i)^{**}$  cannot be a  $k$ -cell for  $k < j-1$ . By Lemma 18 together with (5) we have that  $(xF_j + F_i)^{**}$  cannot be a  $(j-1)$ -cell either and we are finished.  $\square$

**Proposition 21.**  *$F_i$  is a subfield.*

*Proof.* Let  $x \in F_i$ ,  $x \neq 0$ ; our aim is to show that  $xF_i \subset F_i$  (whence  $xF_i = F_i$  since  $F_i$  is finite dimensional). Since  $F_i$  is saturated it is enough to show that  $xF_i S \subset F_i S$ . By contradiction, if  $xF_i S \not\subset F_i S$ , then there exists a linear form  $\sigma$  such that  $\sigma(F_i S) = 0$  but  $\sigma(xF_i S) \neq 0$ . This

last condition translates to  $x \notin F_i^*$  where duality is related to this very choice of non-zero linear form on  $L$ . We would then have  $1 \in F_i^*$  and  $F_i \not\subseteq F_i^*$ . Let us show now that this is not possible.

For  $Z := (F_i + F_i^*)^{**}$ , we have:

$$\partial Z + \partial(F_i \cap F_i^*) \leq \partial(F_i + F_i^*) + \partial(F_i \cap F_i^*) \leq 2\lambda_i.$$

Since we have proved that  $F_i \subset F_j$  for all  $j < i$ , and these inclusions are strict, we have  $F_i^* \supsetneq F_j^*$ , whence  $Z \supsetneq F_j^*$ . Note that  $Z \in \mathcal{S}$  by Lemma 11 (v). Since  $F_j^*$  is a  $j$ -cell whose dual has minimum dimension,  $Z$  cannot be a  $j$ -cell for  $1 \leq j < i$ , otherwise  $Z^*$  would also be a  $j$ -cell, and  $Z^* \subsetneq F_j$  would contradict the minimality of  $F_j$  in  $\mathcal{S}_j$ . By Lemma 12 we also have  $Z \neq L$ , so we conclude that

$$\partial Z \geq \lambda_i.$$

Hence  $\partial(F_i \cap F_i^*) \leq \lambda_i$ , which implies  $F_i \subset F_i^*$  since  $F_i$  is an  $i$ -kernel and has smaller dimension than any  $j$ -cell for  $j < i$  by Proposition 20.  $\square$

We make the passing remark that the proof of Proposition 21 exploits the fact that many different linear forms  $\sigma$  can be used to define duality: this breaks significantly from the additive setting where combinatorial duality is achieved through complementation and can therefore be defined only in a unique way.

**Proposition 22.** *Every  $i$ -cell is stabilized by  $F_i$ .*

*Proof.* Let us suppose that there exists an  $i$ -cell  $X$  that is not stabilized by  $F_i$  and work towards a contradiction. Without loss of generality we may assume that  $X$  is of finite dimension by Corollary 14.

The proof strategy consists in constructing smaller and smaller  $i$ -cells that are not stabilized by  $F_i$  until we eventually exhibit one that is included in  $xF_i$  for some  $x$ , which will yield a contradiction.

That  $X$  is not stabilized by  $F_i$  means there exists  $x \in X$  with  $xF_i \not\subseteq X$ .

We first argue that there exists  $k$ ,  $1 \leq k \leq i-1$ , such that  $X \cap xF_k$  is an  $i$ -cell not stabilized by  $F_i$ .

We have

$$\partial(X + xF_i) + \partial(X \cap xF_i) \leq 2\lambda_i.$$

Since  $X \cap xF_i \subsetneq xF_i$  we have  $\partial(X \cap xF_i) > \lambda_i$ . This is because  $X \cap xF_i$  is a saturated set whose dimension is smaller than that of any  $j$ -cell for  $1 \leq j \leq i$  by Proposition 20. Therefore  $\partial(X + xF_i) < \lambda_i$ . Furthermore, by Lemma 12,  $(X + xF_i)^{**} \neq L$ , so that  $\partial(X + xF_i)^{**} = \lambda_k$  for some  $1 \leq k \leq i-1$ . Now, since  $(X + xF_i)^{**} \in \mathcal{S}_k$  (by Lemma 11 (v)), and  $k < i$ , we know that  $(X + xF_i)^{**} = \widetilde{X + xF_i}$  is stabilized by  $F_k$ , whence

$$(X + xF_i)^{**} = (X + xF_k)^{**}$$

and  $\partial(X + xF_k)^{**} = \lambda_k$ . We now write

$$\partial(X + xF_k)^{**} + \partial(X \cap xF_k) \leq \lambda_k + \lambda_i$$

from which we get  $\partial(X \cap xF_k) \leq \lambda_i$ , which implies  $\partial(X \cap xF_k) = \lambda_i$ , since otherwise  $X \cap xF_k$  is an  $\ell$ -cell for some  $\ell < i$ , and therefore stabilized by  $F_\ell$ , and hence by  $F_i$ , which contradicts our assumption on  $x$ .

The space  $X \cap xF_k$  is therefore an  $i$ -cell that is not stabilized by  $F_i$ , and we may therefore replace  $X$  by an  $i$ -cell which is included in some kernel. Specifically, let  $j \leq i$  be the largest integer such that there exists an  $i$ -cell  $X$  not stabilized by  $F_i$  and included in  $xF_j$  for some  $x \in X$  with  $xF_i \not\subset X$ . Clearly we can only have  $j \leq i - 1$  since there is no  $i$ -cell included in but not equal to  $xF_i$ . We have just shown  $j \geq 1$ . Furthermore, we have also shown that

$$\partial(X + xF_i)^{**} = \lambda_k$$

with  $k \leq j$ ; otherwise, repeating the above argument, there would exist a new  $i$ -cell of the form  $X \cap xF_k$  that is not stabilized by  $F_i$ , which would contradict our definition of  $j$ .

Since  $X + xF_i \subset xF_j$  and  $xF_j$  is saturated, we cannot have  $(X + xF_i)^{**} \in \mathcal{S}_k$  for  $k < j$  as this would imply  $(X + xF_i)^{**} = \widetilde{X + xF_i} \subset xF_j$ , meaning  $xF_j$  contains a  $k$ -cell, which is not possible as a  $j$ -kernel is strictly smaller than a  $k$ -cell for  $k < j$  in view of Proposition 20 and the minimality of  $\dim F_k$  over all  $k$ -cells. Therefore, we have just shown that

$$(X + xF_i)^{**} \in \mathcal{S}_j. \quad (7)$$

Our next objective is to construct an  $i$ -cell that is not stabilized by  $F_i$  and included in a  $(j+1)$ -kernel  $yF_{j+1}$ , which will contradict the definition of  $j$  and prove the proposition. For this we will need to apply Lemma 12 to the space  $X^*$  and to the  $(j+1)$ -kernel, for which we need the condition

$$\dim X \geq \dim F_{j+1} \quad (8)$$

which we now prove. We assume  $j < i - 1$ , since if  $j = i - 1$  (8) is immediate as  $X$  is an  $i$ -cell.

From  $F_{j+1}S \subsetneq F_jS$  (the  $F_j$  are saturated sets) we have, since the  $F_j$  are subfields,

$$\dim F_jS \geq \dim F_{j+1}S + \dim F_{j+1}. \quad (9)$$

For the same reason, since  $F_iS \subsetneq F_{j+1}S$ , we have

$$\dim F_{j+1}S \geq \dim F_iS + \dim F_i. \quad (10)$$

Now from

$$\partial(X + xF_i) + \partial(X \cap xF_i) \leq 2\lambda_i$$

we have  $\partial(X + xF_i) \leq \lambda_i$ , i.e.,

$$\dim(X + xF_i)S - \dim(X + xF_i) \leq \lambda_i$$

meaning

$$\begin{aligned} \dim(X + xF_i)S &\leq \lambda_i + \dim(X + xF_i) \\ &< \lambda_i + \dim X + \dim F_i. \end{aligned} \quad (11)$$

From (7),  $X \subset xF_j$ , and the fact that  $j$ -cells are stabilized by  $F_j$ , we have  $(X + xF_i)S = (X + xF_j)S = xF_jS$ . Writing  $\lambda_i = \dim F_iS - \dim F_i$ , we get from (11)

$$\begin{aligned} \dim F_jS &= \dim(X + xF_i) < \dim F_iS - \dim F_i + \dim X + \dim F_i \\ &\leq \dim F_iS + \dim X \\ &< \dim S + \dim F_i + \dim X. \end{aligned}$$

But on the other hand, (9) and (10) imply

$$\dim F_jS \geq \dim F_iS + \dim F_i + \dim F_{j+1} \geq \dim S + \dim F_i + \dim F_{j+1},$$

whence  $\dim F_{j+1} < \dim X$ .

Now that we have proved (8), we are ready to construct an  $i$ -cell that is not stabilized by  $F_i$  and included in a  $(j+1)$ -kernel  $yF_{j+1}$ .

Since  $X$  is assumed not to be stabilized by  $F_i$ ,  $X^*$  is not stabilized by  $F_i$  either by Corollary 14. Therefore there exists  $y \in X^*$  such that  $yF_i \not\subset X^*$ . We write

$$\partial(X^* + yF_{j+1}) + \partial(X^* \cap yF_{j+1}) \leq \lambda_{j+1} + \lambda_i. \quad (12)$$

By the hypothesis  $X \subsetneq xF_j$ , we have  $X^* + yF_{j+1} \supset X^* \supsetneq (xF_j)^*$ , and  $(X^* + yF_{j+1})^* \subsetneq xF_j$ . Therefore,  $(X^* + yF_{j+1})^*$  and  $(X^* + yF_{j+1})^{**}$  do not belong to  $\mathcal{S}_k$  for any  $1 \leq k \leq j$ . Now (8) and Lemma 12 imply that  $(X^* + yF_{j+1})^{**} \neq L$ . Therefore,

$$\partial(X^* + yF_{j+1}) \geq \lambda_{j+1}.$$

Together with (12) this implies

$$\partial(X^* \cap yF_{j+1}) \leq \lambda_i.$$

If  $X^* \cap yF_{j+1}$  were a  $k$ -cell for  $k < i$ , it would be stabilized by  $F_k$  and hence  $F_i$ : since this is assumed not to be the case, we have that  $X^* \cap yF_{j+1}$  must be an  $i$ -cell. As announced, we have constructed an  $i$ -cell that is included in a  $(j+1)$ -kernel  $yF_{j+1}$ , which contradicts the definition of  $j$ .  $\square$

Propositions 20, 21 and 22 imply that  $i = n$  and prove Theorem 15.

#### 4. PROOF OF THEOREM 3

By replacing  $S$  if need be by  $s^{-1}S$  for some  $s \in S$ , we may always suppose  $1 \in S$ . Suppose first  $L = F(S)$ . If  $T = F(S)$  is the only saturated subspace of finite dimension such that

$$\dim ST < \dim S + \dim T - 1, \quad (13)$$

then the theorem holds with  $K = F(S)$ . Otherwise, if there exists a finite-dimensional subspace  $T$  satisfying (13) and such that  $ST \neq F(S)$ , then we are in the conditions of Theorem 15. In this case  $\tilde{T}$  is a  $k$ -cell for some  $1 \leq k \leq n-1$ , and in particular is stabilized by  $F_k$ , implying that  $ST = S\tilde{T}$  is stabilised by  $F_k$  as well. Since  $F(S)$  and also every space  $F_k$  contain  $F_{n-1}$ , the conclusion of the theorem holds with  $K = F_{n-1}$ .

Consider now the case  $L \supsetneq F(S)$ . Let  $T$  be a subspace satisfying (13).

Let  $t \in T, t \neq 0$ . Let  $T_t = tF(S) \cap T$ : since  $T_t$  is an  $F$ -vector space, we may write  $T = T_t \oplus T'$  for some subspace  $T'$  of  $T$  with  $T' \cap T_t = \{0\}$ . Note that this implies  $T' \cap tF(S) = \{0\}$ . Since  $ST_t \subset tF(S)$ , we have  $ST_t \cap T' = \{0\}$ , and  $ST \supset ST_t \oplus T'$  implies

$$\dim ST \geq \dim ST_t + \dim T'.$$

From

$$\dim S + \dim T_t + \dim T' - 1 = \dim S + \dim T - 1 > \dim ST,$$

we get

$$\dim S + \dim T_t - 1 > \dim ST_t.$$

Now we get from the case  $L = F(S)$  the existence of a subspace  $K$  such that  $ST'K = ST'$  for any subspace  $T'$  satisfying (13) and included in  $F(S)$ , or in a 1-dimensional  $F(S)$ -vector space. Therefore we have  $ST_tK \subset ST$  for every  $t$  which concludes the proof of Theorem 3.

## REFERENCES

- [1] C. BACHOC, O. SERRA, G. ZÉMOR, An analogue of Vosper's Theorem for extension fields, *Math. Proc. Cambridge Philos. Soc.*, to appear. <http://arxiv.org/abs/1501.00602>
- [2] E. BALANDRAUD, Une Variante de la méthode isoperimétrique de Hamidoune appliquée au théorème de Kneser. *Ann. I. Fourier* 58, 915–943 (2008).
- [3] V. BECK AND C. LECOUEVEY, Additive combinatorics methods in associative algebras, preprint (2015) <http://arxiv.org/abs/1504.02287>
- [4] N. BOURBAKI, *Éléments de mathématique*, Livre II, Algèbre, Hermann, 1959.
- [5] J. A. DIAS DA SILVA AND Y. O. HAMIDOUNE, Cyclic spaces for Grassmann derivatives and additive theory, *B. Lond. Math. Soc.* 26, 140–146 (1994).
- [6] S. ELIAHOU AND C. LECOUEVEY, On linear versions of some additive theorems. *Linear Multilinear A.* 57, 759–775 (2009).
- [7] In memory of Yahya Ould Hamidoune, special issue of European Journal of Combinatorics, Plagne, Serra and Zémor Eds., Vol. 34, 2013.
- [8] X. HOU, On a vector space analogue of Kneser's theorem. *Linear Algebra Appl.* 426, 214–227 (2007).
- [9] X. HOU, K.H. LEUNG, AND Q. XIANG, A generalization of an addition theorem of Kneser. *J. Number Theory* 97, 1–9 (2002).
- [10] GYULA KÁROLYI, The Erdős-Heilbronn problem in Abelian groups. *Isr. J. Math.* 139, 349–359 (2004).
- [11] J.H.B. KEMPERMAN, On complexes in a semigroup. *Indagationes Mathematicae (Proceedings)* 18, 247–254 (1956).
- [12] M. KNESER, Summenmengen in lokalkompakten abelschen Gruppen. *Math. Z.* 66, 88–110 (1956).
- [13] S. LANG, *Algebra*, Springer, 3rd Edition, (2005).
- [14] C. LECOUEVEY, Plünnecke and Kneser type theorems for dimension estimates. *Combinatorica* 34, 331–358 (2014).
- [15] M.B. NATHANSON, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.
- [16] J.E. OLSON, On the sum of two sets in a group. *J. Number Theory* 18, 110–120 (1984).
- [17] A. PLAGNE, O. SERRA AND G. ZÉMOR, Yahya Ould Hamidoune's mathematical journey: A critical review of his work. *European Journal of Combinatorics*, 34, 1207–1222 (2013).
- [18] I.Z. RUZSA, An application of graph theory to additive number theory. *Scientia. Series A: Mathematical Sciences* 3, 97–109 (1989).
- [19] T. TAO AND V. VU, *Additive Combinatorics*, Cambridge University Press, 2006.



INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UMR 5251, UNIVERSITÉ DE BORDEAUX, 351 COURS DE LA LIBÉRATION, 33400 TALENCE, FRANCE.

*E-mail address:* `Christine.Bachoc@math.u-bordeaux.fr`

DEPARTMENT OF MATHEMATICS, UNIVERSITAT POLITÈCNICA DE CATALUNYA AND BARCELONA GRADUATE SCHOOL OF MATHEMATICS, BARCELONA, SPAIN.

*E-mail address:* `oriol.serra@upc.edu`

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UMR 5251, UNIVERSITÉ DE BORDEAUX, 351 COURS DE LA LIBÉRATION, 33400 TALENCE, FRANCE.

*E-mail address:* `zemor@math.u-bordeaux.fr`