

# Towards a function field version of Freiman's Theorem

Christine Bachoc\* and Alain Couvreur<sup>†</sup> and Gilles Zémor\*

September 1, 2017

## Abstract

We discuss a multiplicative counterpart of Freiman's  $3k - 4$  theorem in the context of a function field  $F$  over an algebraically closed field  $K$ . Such a theorem would give a precise description of subspaces  $S$ , such that the space  $S^2$  spanned by products of elements of  $S$  satisfies  $\dim S^2 \leq 3 \dim S - 4$ . We make a step in this direction by giving a complete characterisation of spaces  $S$  such that  $\dim S^2 = 2 \dim S$ . We show that, up to multiplication by a constant field element, such a space  $S$  is included in a function field of genus 0 or 1. In particular if the genus is 1 then this space is a Riemann-Roch space.

## 1 Introduction

We are interested in linear analogues of addition theorems that occur in field extensions  $F/K$  of a base field  $K$ . If  $S$  and  $T$  are finite-dimensional  $K$ -vector subspaces of  $F$ , we denote by  $ST$  the  $K$ -linear span of the set of all products  $st$ ,  $s \in S$ ,  $t \in T$ . The general purpose of this area of research is to characterise subspaces  $S$  and  $T$  whose product  $ST$  has unusually small dimension: it is naturally inspired by one of the goals of additive combinatorics which is to characterise subsets  $A, B$  of elements of a group that have sumsets  $A + B$  of small cardinality, where  $A + B$  denotes the set of elements  $a + b$ ,  $a \in A$ ,  $b \in B$ .

The first significant result in this direction is arguably due to Hou, Leung and Xiang [9] and generalises the classical addition theorem of Kneser [8]. It essentially states that if  $\dim ST < \dim S + \dim T - 1$ , then the space  $ST$  must be stabilised by a non-trivial subfield of  $F$ . A welcome feature of Hou et al.'s theorem is that Kneser's original theorem can be recovered from it, so that it is not only a transposition to the linear setting of its additive counterpart, but it can also be seen as a generalisation. Hou's Theorem was finally proved for all field extensions in [2], and also studied in other algebras than field extensions [3, 10]. Linear versions of addition theorems were also studied in the somewhat broader context of skew field extensions in [5].

A common feature of the above works is that they tend to focus on highlighting the existence of finite dimensional subfields or subalgebras, whenever  $\dim ST < \dim S + \dim T - 1$ . In contrast, in [1] field extensions  $F/K$  are studied where there are no subextensions of  $K$  in  $F$  ( $K$  is algebraically closed in  $F$ ) in which case one always has  $\dim ST \geq \dim S + \dim T - 1$  whenever  $ST \neq F$  [5]. The goal of [1] was to prove that the equality

---

\*Institut de Mathématiques de Bordeaux, CNRS UMR 5251, Université de Bordeaux, 351 cours de la Libération, 33400 Talence.

<sup>†</sup>INRIA & Laboratoire LIX, CNRS UMR 7161, École Polytechnique, Université Paris Saclay, 91128 Palaiseau Cedex

$\dim ST = \dim S + \dim T - 1$  essentially implies that  $S$  and  $T$  have bases in geometric progression: this is a linear equivalent of Vosper's Theorem [15] which states that in a group of prime order, or more generally an abelian group with no finite subgroups,  $|A + B| = |A| + |B| - 1$  implies that  $A$  and  $B$  are arithmetic progressions (with some degenerate cases ruled out). It is proved in [1] that a linear version of Vosper's theorem holds when the base field  $K$  is finite, and for a number of other base fields, but not for every field  $K$ , even if it is assumed to be algebraically closed in  $F$ .

A particularly simple case for which a linear version of Vosper's Theorem can be derived from an addition theorem, is when the base field  $K$  is itself assumed to be algebraically closed. The linear theorem then follows almost directly from considering sets  $A$  and  $B$  of valuations of the field elements in  $S$  and  $T$  and arguing that  $A$  and  $B$  must satisfy an addition theorem. From this perspective it becomes very natural to ask what can be said of the structure of spaces  $S$  such that

$$\dim S^2 = 2 \dim S - 1 + \gamma \tag{1}$$

for increasing values of  $\gamma$ . We have switched to the symmetric situation  $S = T$  for the sake of simplicity.

In the additive case, recall Freiman's "3k - 4" Theorem [6], [14, Th. 5.11], which says that in a torsion-free abelian group,

$$|A + A| = 2|A| - 1 + \gamma$$

implies, when  $\gamma \leq |A| - 3$ , that  $A$  is included in an arithmetic progression of length  $|A| + \gamma$  (i.e.  $A$  is a progression with at most  $\gamma$  missing elements). Candidates for spaces  $S$  satisfying (1) are of course subspaces (of codimension at most  $\gamma$ ) inside a space that has a basis in geometric progression. However, some thought yields alternative spaces that do not have an additive analogue when  $\gamma \geq 1$ : namely Riemann-Roch spaces  $L(D)$  of an algebraic curve of genus  $\gamma$ , which are easily seen to satisfy (1). It is tempting to conjecture that, in the case when the base field  $K$  is algebraically closed, any space satisfying (1) is, up to multiplication by a constant, a subspace of codimension  $t$  inside a Riemann-Roch space of an algebraic curve of genus  $g$ , with  $t + g \leq \gamma$ . With this in mind, let us call the quantity  $\gamma$  in (1) the *combinatorial genus* of  $S$ . In the present paper we make a modest contribution towards this hypothesis by proving it in the case when  $\gamma = 1$ .

We will use a blend of combinatorial and algebraic methods. The paper is organised as follows: Section 2 recalls basic properties of valuations that will in particular associate sets of integers with small sumsets to subspaces with products of small dimension. Section 3 proves an extension field version of "Freiman's Lemma" where the transcendence degree plays a role analogous to the rank of a set of elements of a torsion-free abelian group. Section 4 introduces a lattice of subspaces that we shall rely on heavily, and illustrates its usefulness by characterising spaces with combinatorial genus equal to zero. Section 5 recalls basic properties of Riemann-Roch spaces and states the paper's main result, Theorem 5.3. Section 6 proves Theorem 5.3. Finally, Section 7 complements Theorem 5.3 by giving a precise characterisation of those subspaces of Riemann-Roch spaces that have combinatorial genus equal to 1.

## 2 Valuations

We start by recalling some basic facts about valuations in function fields that will be crucial to transferring additive statements to the extension field setting.

Let  $K$  be a field, a *function field in  $m$  variables over  $K$*  is a field  $F$  which is a finitely generated algebra of transcendence degree  $m$ . Equivalently it is a finite extension of the field  $K(X_1, \dots, X_m)$  of rational fractions in  $m$  variables.

We recall that such fields have *valuations* that map  $F^\times$  to the elements of some ordered group. Valuations are multiplicative, i.e.  $v(xy) = v(x) + v(y)$  and satisfy the ultrametric inequality,  $v(x + y) \geq \min\{v(x), v(y)\}$  with equality when  $v(x) \neq v(y)$ . The map  $v$  is extended to  $F$  with the convention  $v(0) = \infty$ .

Valuations come with *valuation rings*  $\mathcal{O} \subset F$  and with maximal ideal  $\mathfrak{m}$  and residue field  $\mathcal{O}/\mathfrak{m}$ . We refer the reader to [4, Ch. 6] for further details.

Let  $S \subseteq F$  be a finite dimensional  $K$ -vector space of dimension  $n > 0$ . Given a valuation  $v$  on  $F$  with residue field  $K$ , we denote by  $v(S)$  the set of valuations of the non-zero elements of  $S$ . We recall the following classical result, and give a proof for the sake of self-containedness.

**Proposition 2.1.** *The set  $v(S)$  is finite and its cardinality equals  $\dim S$ . Moreover, there exists a basis  $(e_1, \dots, e_n)$  of  $S$  such that*

$$v(e_1) > v(e_2) > \dots > v(e_n) \quad \text{and} \quad \{v(e_1), \dots, v(e_n)\} = v(S).$$

Such a basis is referred to as a filtered basis.

*Proof.* First notice that elements of  $F$  with distinct finite valuations are linearly independent. Indeed, if  $x_1, \dots, x_k$  have distinct valuations, then so do  $a_1x_1, \dots, a_kx_k$  for non-zero  $a_i \in K$ , since non-zero elements of  $K$  have valuation 0, so that  $v(a_1x_1 + \dots + a_kx_k) = \min(v(x_1), \dots, v(x_k))$  must be finite, meaning  $a_1x_1 + \dots + a_kx_k$  must be non-zero. This shows that  $|v(S)| \leq \dim S$ .

Now let  $E$  be a subspace of  $S$  such that  $v(E) = v(S)$  and suppose  $E \subsetneq S$ . Let  $x$  be an element of  $S \setminus E$  with maximal valuation in  $\{v(s), s \in S \setminus E\}$ . Let  $e \in E$  be such that  $v(e) = v(x)$ . Then,  $xe^{-1} \in \mathcal{O}^\times$  and since the residue field is  $K$ , there exists  $\lambda \in K$  such that  $xe^{-1} \equiv \lambda \pmod{\mathfrak{m}}$ . Therefore,  $x - \lambda e$  has a valuation larger than  $v(x)$ , a contradiction. Therefore  $E = S$ , meaning that we have  $\dim S = |v(S)|$ . Choosing any  $n$  elements of  $S$  with distinct finite valuations yields a filtered basis.  $\square$

The following lemma is elementary but fundamental to the study of the structure of products  $S^2$  of small dimension. It enables us to involve theorems from additive combinatorics.

**Lemma 2.2.** *For any valuation  $v$  on  $F$ , and any  $K$ -subspace  $S$ ,*

$$v(S) + v(S) \subseteq v(S^2). \tag{2}$$

*Remark 2.3.* Note that this inclusion is not necessarily an equality. For instance, consider the subspace  $H$  of  $K(x)$  of basis  $1, x, x^2, x^3 + \frac{1}{x}$  and the valuation  $v$  at infinity. Then  $v(H) = \{0, -1, -2, -3\}$  while  $H^2 = \langle \frac{1}{x}, 1, x, x^2, \dots, x^5, x^6 + \frac{1}{x^2} \rangle$  whose valuation set contains  $v(1/x) = 1$  which is not in  $v(H) + v(H)$ .

### 3 Transposing Freiman's Lemma in field extensions

Recall the following result of Freiman [6], named "Freiman's Lemma" by Tao and Vu [14, Lemma 5.13].

**Theorem 3.1.** *Let  $A$  be a finite subset of  $\mathbf{R}^d$  such that no hyperplane of  $\mathbf{R}^d$  contains a translate of  $A$ . Then*

$$|A + A| \geq (d + 1)|A| - d(d + 1)/2.$$

Let  $S$  be a  $K$ -vector space inside a field extension  $L$  of a field  $K$ . We remark that for a non-zero element  $s$  of  $S$ , the field subextension  $K(Ss^{-1})$  of  $L$  is independent of the choice of the element  $s$ . Let us call the *transcendence degree* of  $S$  the transcendence degree of  $K(Ss^{-1})$  over  $K$ . Similarly, by the *genus* of  $S$  we will mean the genus of the field extension  $K(Ss^{-1})/K$  (see Theorem 5.3 in Section 5.2).

We have the extension field analogue of Theorem 3.1:

**Theorem 3.2.** *Let  $K$  be a perfect field and let  $F \supseteq K$  be an extension field of  $K$  such that  $K$  is algebraically closed in  $F$ . Let  $S$  be a  $K$ -vector subspace of  $F$  of finite dimension and of transcendence degree  $d$ . Then*

$$\dim S^2 \geq (d + 1) \dim S - d(d + 1)/2.$$

The proof of Theorem 3.2 rests upon the following lemma.

**Lemma 3.3.** *If  $F/K$  is a field extension over an algebraically closed field  $K$ , and if  $x_1, \dots, x_d$  are  $K$ -algebraically independent elements of  $F$  such that  $F$  is an algebraic extension of  $K(x_1, \dots, x_d)$ , then there exists a valuation  $v$  of  $F$ , such that the associated valuation ring has residue field isomorphic to  $K$  and such that the valuation values  $v(x_1), v(x_2), \dots, v(x_d)$  generate a group isomorphic to  $\mathbf{Z}^d$ .*

*Proof.* It is standard to construct a valuation  $v$  from  $K(x_1, x_2, \dots, x_d)$  to  $\mathbf{Z}^d$  such that  $v(x_1) = (1, 0, \dots, 0), v(x_2) = (0, 1, \dots, 0), \dots, v(x_d) = (0, \dots, 0, 1)$  and with associated residue field isomorphic to  $K$  (see e.g. [4, Ch. 6, §3.4, Example 6]). This valuation can then be extended to the whole of  $F$  [4, Ch. 6, §3.3, Proposition 5] with its residue field necessarily becoming an algebraic extension of the original residue field associated to  $v$  [4, Ch. 6, §8.1, Proposition 1]. Since  $K$  is algebraically closed, the residue field associated to the extended valuation must therefore also be isomorphic to  $K$ .  $\square$

*Proof of Theorem 3.2.* Without loss of generality we may suppose  $K \subset S$  and  $F = K(S)$ .

First suppose that  $K$  is algebraically closed. Let  $x_1, \dots, x_d$  be  $d$  algebraically independent elements of  $F$ . Choose for  $v$  a valuation given by Lemma 3.3. Then, since the residue field associated to  $v$  is  $K$ , by Proposition 2.1 we know that  $\dim S = |v(S)|$  and  $\dim S^2 = |v(S^2)|$ . From (2) we have  $\dim S^2 \geq |v(S) + v(S)|$  and Theorem 3.1 now gives us

$$|v(S) + v(S)| \geq (d + 1)|v(S)| - d(d + 1)/2 = (d + 1) \dim S - d(d + 1)/2$$

which proves the theorem in the case when  $K$  is algebraically closed.

Now consider the general case when  $K$  is only supposed to be a perfect field and algebraically closed in  $F$ . Let  $K'$  be an algebraic closure of  $K$  and  $F' = K'(S)$  be defined inside the algebraic closure of  $F$ . It holds that any  $K$ -linearly independent elements of  $F$  are also  $K'$ -linearly independent in  $F'$  ([13, Proposition III.6.1]<sup>1</sup>). Therefore  $\dim_K S = \dim_{K'} K'S$  and  $\dim_K S^2 = \dim_{K'} K'S^2$ , and the theorem is proved by arguing that the transcendence degree of  $S$  is the same over  $K'$  as over  $K$ , and that therefore

$$\dim_{K'} K'S^2 \geq (d + 1) \dim_{K'} K'S - d(d + 1)/2$$

by applying the theorem in the algebraically closed field case.  $\square$

<sup>1</sup>The context of the proposition is that of functions fields of one variable, but its proof applies verbatim to arbitrary field extensions.

*Remark 3.4.* Actually the hypothesis “ $K$  is perfect” can be relaxed to “any finite extension of  $K$  is generated by a single element”. The result holds for instance when  $K = \mathbf{F}_q(t)$ . On the other hand if the condition is not satisfied, then it is not necessarily the case that  $K$ -linearly independent elements of  $S$  stay linearly independent over an algebraic extension of  $K$ , in which case the argument in the above proof breaks down. Whether Theorem 3.2 continues to hold for an arbitrary field  $K$  remains therefore an open question.

**Consequence.** When one considers a space  $S$ ,  $K \subset S \subset F$ , with  $\dim S^2 \leq 3 \dim S - 4$ , and  $F = K(S)$ , then  $F$  is a function field in one variable. In particular, from [13, Theorem 1.1.16], every valuation on  $F$  is discrete and its set of values is  $\mathbf{Z}$ .

For the rest of this paper we will assume this setting, namely a sufficiently small combinatorial genus  $\gamma$ , so that the transcendence degree of  $S$  can only be equal to 1. The term *function field* will consequently always mean from now on *function field in one variable*. Since the multiplicative properties of  $S$  that we wish to study are invariant by multiplication by a constant non-zero element, it will also be convenient to systematically assume  $1 \in S$ , so that  $K(S)$  is a function field (in one variable). We will indifferently refer to valuations or to the associated places they correspond to. We will also stop trying to deal with the most general base fields  $K$ , and assume  $K$  algebraically closed, which implies in particular that all places have residue fields equal to  $K$ .

## 4 Products of spaces, the lattice of subspaces and characterising spaces with combinatorial genus $\gamma = 0$

In order to study the structure of a product set  $S^2$ , the lattice of subspaces that we introduce below will be particularly useful. Its structure will enable us to almost immediately characterise spaces with the smallest possible combinatorial genus.

### 4.1 The lattice of subspaces

Let  $(e_1, \dots, e_n)$  be a filtered basis of the space  $S$  relative to a valuation  $v$  associated to a place  $P$ . Consider the sequence of subspaces

$$S_1 \subset S_2 \subset \dots \subset S_n = S$$

where  $S_i$  denotes the subspace of  $S$  generated by  $e_1, \dots, e_i$ . We will also refer to this sequence of spaces as the *filtration of  $S$  relative to  $P$* . We note that these spaces are independent of the choice of the specific filtered basis used to define them.

Since dimensions of spaces are unchanged by multiplication by a constant element, we may assume  $e_1 = 1$  and  $S_1 = K$ . It will be useful to consider the lattice of subspaces of  $S^2$  consisting of the products of subspaces  $S_i S_j$  and ordered by inclusion, as represented on Figure 1. We will consider directed edges between  $S_i S_j$  and  $S_i S_{j+1}$  and between  $S_i S_j$  and  $S_{i+1} S_j$ , and label both edges by a weight defined as the codimension of  $S_i S_j$  inside  $S_i S_{j+1}$  and  $S_{i+1} S_j$  respectively. We will make several times the argument that the sum of weights on two directed paths that lead from the same initial vertex to the same terminal vertex must be the same because they both equal the codimension of the initial subspace inside the terminal subspace. Notice also that all weights must be positive because the valuation set of an initial subspace must be strictly smaller than the valuation set of the corresponding terminal subspace: indeed,  $e_i e_{j+1}$  is an element of minimal valuation of  $S_i S_{j+1}$  that cannot belong to  $S_i S_j$  because the minimum of  $v(S_i S_j)$  is attained by  $e_i e_j$ , and similarly for  $S_{i+1} S_j$ .

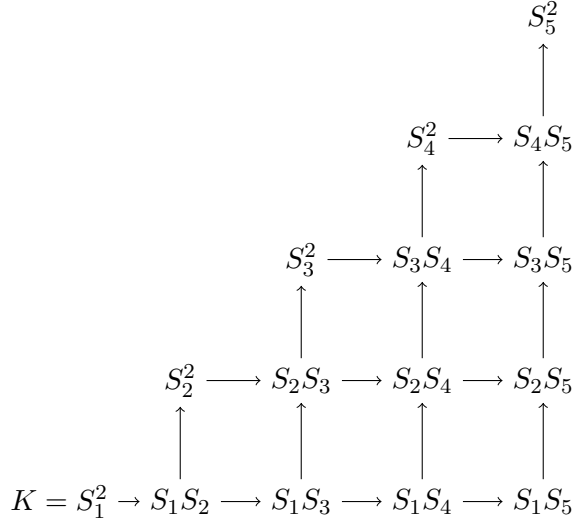


Figure 1: the lattice of subspaces

The following Lemma states that when two edges that fall into the same terminal vertex both have weight 1, then the initial vertices correspond to the same subspace.

**Lemma 4.1.** *Suppose the spaces  $S_iS_{j+1}$  and  $S_{i+1}S_j$  both have codimension 1 inside  $S_{i+1}S_{j+1}$ , then  $S_iS_{j+1} = S_{i+1}S_j$ .*

*Proof.* Let  $U = \{s \in S_{i+1}S_{j+1}, v(s) > \min v(S_{i+1}S_{j+1})\}$ . We have that  $U \subsetneq S_{i+1}S_{j+1}$  and  $U$  is a subspace containing both  $S_iS_{j+1}$  and  $S_{i+1}S_j$  which must therefore all have the same dimension and be equal.  $\square$

## 4.2 The structure of $S$ when $\gamma = 0$

Like in the previous subsection we assume that  $e_1 = 1$ , and we moreover set  $x = e_2$ .

**Lemma 4.2.** *Suppose all directed edges lying on any path from  $S_1$  to  $S_iS_j$ ,  $2 \leq i$ , have weight 1. Then for every  $k$ ,  $2 \leq k \leq j$ , the space  $S_k$  is generated by  $1, x, x^2, \dots, x^{k-1}$ .*

*Proof.* Proceed by induction on  $k$ . Suppose the result is proved for  $k$  and prove it for  $k+1 \leq j$ . By applying Lemma 4.1 to  $S_1S_{k+1}$  and  $S_2S_k$  inside  $S_2S_{k+1}$ , we obtain  $S_{k+1} = \langle 1, x \rangle S_k$  meaning that  $S_{k+1}$  is generated by  $(1, x, x^2, \dots, x^k)$ .  $\square$

As an immediate corollary we obtain the following theorem, which is proved in [1] in more generality. Its proof illustrates the usefulness of the subspace lattice described above.

**Theorem 4.3.** *Let  $K$  be an algebraically closed field, and let  $S$  be a finite-dimensional  $K$ -vector space lying in a field extension  $F$  of  $K$ . If  $\dim S^2 = 2 \dim S - 1$  then  $S$  has a basis in geometric progression, i.e. of the form  $(a, ax, ax^2, \dots, ax^{n-1})$ .*

*Proof.* Replacing  $S$  by  $e_1^{-1}S$  reduces to the case  $e_1 = 1$ . Because the codimension of  $K$  in  $S^2$  is  $2 \dim S - 2$  and is equal to the length of any path from  $K$  to  $S^2$  in the lattice, we have that every edge must be of weight 1. The result therefore follows from Lemma 4.2.  $\square$

We now turn to Riemann-Roch spaces that provide more spaces of low combinatorial genus  $\gamma$ .

## 5 Divisors, Riemann-Roch spaces, and characterising spaces with combinatorial genus $\gamma = 1$

### 5.1 Divisors and Riemann-Roch spaces on function fields

We quickly recall some basic notions on the theory of the function fields in one variable (or equivalently of algebraic curves). For further details, we refer the reader to [13] or to [7] for a more geometric point of view.

Let  $K$  be an algebraically closed field and let  $F$  be a function field over  $K$ . A *divisor on  $F$*  is an element of the free abelian group generated by the places of  $F$ . Thus it is a formal  $\mathbf{Z}$ -linear combination of places. Given a function  $f \in F^\times$ , the divisor of  $f$  is defined as

$$(f) := \sum_{P \text{ place of } F} v_P(f)P$$

where  $v_P$  denotes the valuation associated to the place  $P$ . The group of divisors is partially ordered as follows: given a divisor  $G = g_1P_1 + \dots + g_mP_m$ , we have  $G \geq 0$  if  $g_1, \dots, g_m \geq 0$ . Next  $G \geq H$  if  $G - H \geq 0$ .

Given a divisor  $D$  of  $F$ , the Riemann-Roch space  $L(D)$  is defined as

$$L(D) := \{f \in F \mid (f) + D \geq 0\} \cup \{0\}.$$

The dimension of this space is given by the famous Riemann-Roch theorem [13, Theorem 1.5.15]. In particular it satisfies:

$$\text{If } \deg D > 2g - 2 \text{ then } \dim L(D) = \deg(D) + 1 - g$$

where  $g$  denotes the *genus* of the field  $F$ .

Two divisors  $D, D'$  are said to be *linearly equivalent* which we denote by  $D \sim D'$  if  $D' = D + (f)$  for some function  $f \in F^\times$ . Such an equivalence induces an isomorphism between the Riemann-Roch spaces which is explicit:

$$\begin{array}{ccc} L(D') & \longrightarrow & L(D) \\ s & \longmapsto & fs. \end{array}$$

In short  $L(D) = fL(D')$ .

The following well-known result due to Mumford gives an explicit formula for the product of Riemann-Roch spaces.

**Theorem 5.1** ([11, Theorem 6]). *Let  $D, D'$  be two divisors of a function field  $F$  of genus  $g$ . Suppose that  $\deg D \geq 2g$  and  $\deg D' \geq 2g + 1$ . Then*

$$L(D)L(D') = L(D + D').$$

In particular, combining the Riemann-Roch theorem with Theorem 5.1, one has that in a function field of genus  $g$ , for any divisor  $D$  of degree larger than  $2g + 1$ , the space  $L(D)$  has combinatorial genus  $\gamma = g$ .

Finally, recall that a function field  $F$  has genus 0 if and only if it is a purely transcendental extension  $F = K(x)$  of  $K$ . In such an extension, the space generated by the functions  $1, x, x^2, \dots, x^n$  is equal to the Riemann-Roch space  $L(nP_\infty)$  where  $P_\infty$  is the place at infinity. We remark that the statement of Theorem 4.3 is equivalent to saying that a space  $S$  has combinatorial genus  $\gamma = 0$  if and only if it has genus 0 and is equal to a Riemann-Roch space  $L(D) = aL(nP_\infty)$  for a divisor  $D = nP_\infty - (a)$  and a function  $a$ .

## 5.2 Statement of the main theorem

Our main purpose is to classify spaces over  $K$  with combinatorial genus 1. That is to say, given a finitely generated field  $F$  over  $K$  we want to understand the structure of  $K$ -spaces  $S \subseteq F$  such that  $\dim S^2 = 2 \dim S$ . As remarked at the end of Section 3, we know from Theorem 3.2 that the degree of transcendence of  $S$  must be equal to 1, so that, assuming without loss of generality  $1 \in S$ ,  $F$  is a function field (in one variable).

With the case  $\gamma = 1$  in mind, we recall for future reference its additive analogue:

**Proposition 5.2.** *A subset  $A$  of the integers,  $|A| \geq 4$ , is such that  $|A + A| = 2|A|$  if and only if it is of the form  $A = a + \{0, 2d, 3d, \dots, (n-1)d, nd\}$  for some non-zero  $d$ : in other words, writing  $A$  as an increasing sequence, it is an arithmetic progression with a missing element after the first position (positive  $d$ ) or before the last position (negative  $d$ ).*

Indeed, Freiman's  $3k - 4$  Theorem applied to the case  $|A + A| = 2|A|$  gives that  $A$  is an arithmetic progression with a single missing element, which is then easily seen to be necessarily at an extreme end of the progression.

To generate a space  $S$  such that  $\gamma = 1$ , Proposition 5.2 suggests naturally to take a basis of the form  $x^a, a \in A$ , where  $A$  is such that  $|A + A| = 2|A|$ . Such a space is a subspace of codimension 1 inside a space with a basis in geometric progression, i.e. inside a Riemann-Roch space of genus 0.

Alternatively, Theorem 5.1 tells us that Riemann-Roch spaces of genus 1 will also give us spaces with combinatorial genus equal to 1.

Our main result states, broadly speaking, that the two constructions above exhaust all possible cases:

**Theorem 5.3.** *Let  $S \subseteq F$ ,  $1 \in S$ , be a space of finite dimension  $n \geq 4$  and combinatorial genus  $\gamma = 1$ . Then  $S$  has genus 0 or 1. Moreover,*

- *if  $S$  has genus 1 then  $S = L(D)$  for  $D$  a divisor of degree  $n$ ,*
- *if  $S$  has genus 0, then  $S$  is a subspace of codimension 1 inside a space  $L(D)$  for  $D$  a divisor of degree  $n$ .*

We remark that in the genus  $g = 0$  case, all subspaces of codimension 1 inside an  $L(D)$  space do not necessarily have combinatorial genus  $\gamma$  equal to 1. We postpone to Section 7 the precise characterisation of such subspaces which is slightly more involved than in the additive case given by Proposition 5.2.

## 6 Proof of Theorem 5.3

### 6.1 Overview

Since the proof of the Theorem is somewhat lengthy, we give an outline.

As we have argued before, we may always assume that  $1 \in S$ , and that  $F = K(S)$ . We start by fixing an arbitrary place  $P$  and an associated  $P$ -filtered basis which, possibly after replacing  $S$  by a multiplicative translate  $s^{-1}S$ , is of the form

$$e_1 = 1, e_2 = x, e_3 = y, \dots, e_n$$

with valuations in decreasing order  $v_P(1) = 0 > v_P(x) > v_P(y) > \dots > v_P(e_n)$ .

Next we define (Section 6.2) the divisor  $D_U$  of a space  $U$  to be the smallest Riemann-Roch space that contains  $U$ . Our strategy will be to study closely the chain of divisors



$D_{S_i}$  for the filtration  $(S_i)$  of  $S$  relative to  $P$ . Our goal will be to show that  $S_i$  is either equal to  $L(D_{S_i})$  or of codimension 1 inside  $L(D_{S_i})$ , for all  $i \geq 2$ .

We will consider closely the lattice of subspaces introduced in Section 4.1 and exploit the fact that most of its edges are of weight 1. A crucial intermediate result will be Lemma 6.10 which will tell us that the divisor increments  $D_{S_{i+1}} - D_{S_i}$  must all be equal to  $D_{S_3} - D_{S_2}$ , except possibly for one index  $i$ , that we call the  $P$ -index of  $S$ , which is the unique index  $i$  for which  $\dim S_i S_{i+1} > \dim S_i^2 + 1$ . Sections 6.3 and 6.4 build up material leading up to Section 6.5 which derives Lemma 6.10.

Section 6.6 considers next the algebraic equations satisfied by  $x$  and  $y$ . We will show that  $F = K(S) = K(x, y)$  and that  $F$  must be of genus  $g \leq 1$ . We then turn to determining the sequence  $(D_{S_i})$  exactly. Lemma 6.10 tells us that when the  $P$ -index equals 2, the divisors  $D_{S_2}$  and  $D_{S_3}$  determine the whole sequence. In Section 6.7 we show that in this case we must have  $D_{S_2} = P + Q$  and  $D_{S_3} = 2P + Q$  for some place  $Q$  (possibly equal to  $P$ ), so that the whole sequence of divisors must take the form  $0, P + Q, 2P + Q, 3P + Q, \dots, (n-1)P + Q$ . Section 6.8 deals with the remaining case, for which it is shown that the sequence of divisors must be of the form  $0, P, 2P, \dots, (n-2)P, (n-1)P + Q$ .

## 6.2 Minimum valuations, the divisor of a space

The following lemma is straightforward:

**Lemma 6.1.** *Let  $U, V$  be two finite dimensional  $K$ -spaces in  $F$ . Let  $v$  be a valuation on  $F$ . Then,  $\min v(UV) = \min v(U) + \min v(V)$ .*

Note that  $\min v(U) = 0$  for all valuations  $v$  on  $F$  but finitely many of them. This justifies the following:

**Definition 6.2.** we denote by  $D_U$  the divisor

$$D_U := \sum_{P, \text{ place of } F} -\min v_P(U)P.$$

This is the smallest divisor  $D$  such that  $U \subseteq L(D)$ .

## 6.3 Separation

**Definition 6.3** (Separation). Given a finite dimensional  $K$ -space  $U \subset F$  and two distinct places  $P_1$  and  $P_2$ , one says that  $U$  separates  $P_1$  and  $P_2$  if there exists  $f_1, f_2 \in U$  such that

- (i)  $v_{P_i}(f_i) = \min v_{P_i}(U)$  for  $i \in \{1, 2\}$ ;
- (ii) for  $i \neq j \in \{1, 2\}$ ,  $v_{P_i}(f_j) > \min v_{P_i}(U)$ .

Given a  $K$ -space  $U \subset F$  and a place  $P$ , let  $U_P := \{u \in U \mid v_P(u) > \min v_P(U)\}$ . Such a space has codimension 1 in  $U$  and the notion of separation of two distinct places can be reformulated as follows.

**Lemma 6.4.** *The space  $U$  separates two distinct places  $P, Q$  if and only if  $U_P \neq U_Q$ .*

A first example of spaces having a good property of separation are Riemann-Roch spaces. The following statement is classical, we provide a proof for the sake of self-containedness.

**Lemma 6.5.** *Let  $F$  be a function field of genus  $g$  and let  $D$  be a divisor of  $F$  such that  $\deg D > 2g$ . Then the space  $L(D)$  separates any two places  $P$  and  $Q$ .*

*Proof.* Since  $\deg(D) > 2g$ , we have as a consequence of the Riemann-Roch Theorem

$$\begin{aligned}\dim L(D - Q) &= \dim L(D) - 1 \\ \dim L(D - P) &= \dim L(D) - 1 \\ \dim L(D - P - Q) &= \dim L(D) - 2.\end{aligned}$$

Indeed, all the considered divisors have degree greater than  $2g - 2$ . If we set  $U = L(D)$  we get  $U_P \neq U_Q$  and conclude using Lemma 6.4.  $\square$

The next lemma deals with separation in products of spaces.

**Lemma 6.6.** *Let  $U, V \subseteq F$  be two  $K$ -spaces and  $P, Q$  two places of  $F$ . Then,  $UV$  separates  $P$  and  $Q$  if and only if  $U$  or  $V$  separates  $P$  and  $Q$ .*

*Proof.* Let us suppose first that  $U$  separates  $P$  and  $Q$ . Let  $a \in U$  be such that  $v_P(a) = \min v_P(U)$  and  $v_Q(a) > \min v_Q(U)$ . Let  $b \in V$  be such that  $v_P(b) = \min v_P(V)$ . We have  $ab \in (UV)_Q \setminus (UV)_P$ , hence  $UV$  separates  $P$  and  $Q$ .

Conversely, suppose that neither  $U$  nor  $V$  separates  $P$  and  $Q$ . Let  $u \in U$  and  $v \in V$  be such that

$$U = U_P \oplus Ku \quad \text{and} \quad V = V_P \oplus Kv.$$

Then,

$$UV = (U_P V_P + uV_P + U_P v) + Kuv.$$

Clearly  $(U_P V_P + uV_P + U_P v) \subseteq (UV)_P$  and since  $(U_P V_P + uV_P + U_P v)$  has codimension at most 1 in  $UV$  we conclude that

$$(U_P V_P + uV_P + U_P v) = (UV)_P.$$

By assumption, we have  $U_P = U_Q$  and  $V_P = V_Q$  and hence

$$(UV)_P = U_Q V_Q + uV_Q + U_Q v = (UV)_Q$$

so  $UV$  does not separate  $P$  and  $Q$  either. This concludes the proof.  $\square$

#### 6.4 The lattice of subspaces and the $P$ -index of a space

For the remainder of Section 6,  $P$  is a fixed arbitrary place of  $F = K(S)$ . We choose a filtered basis  $(e_1, \dots, e_n)$  where, having replaced  $S$  by  $e_1^{-1}S$  if necessary, we have set  $e_1 = 1$ . We consider the filtration  $S_1 \subset S_2 \subset \dots \subset S_n = S$  associated to  $P$ , together with the lattice of subspaces  $S_i S_j$  introduced in Section 4.1 and illustrated in Figure 1. Recall that the weight of an edge  $V \rightarrow W$  is given by the codimension of  $V$  in  $W$ . In the case  $\dim S^2 = 2 \dim S$  we have:

**Lemma 6.7.** *All edges lying on a directed path from  $S_1^2$  to  $S_n^2 = S^2$  have weight 1 except for an edge which has weight 2.*

*Proof.* The path has  $2n - 2$  edges, while  $\dim S_1^2 = 1$  and  $\dim S_n^2 = \dim S^2 = 2n$ , therefore the codimension of  $S_1^2$  in  $S_n^2$ , which is also the sum of weights on the path, equals  $2n - 1$ . Remembering that weights are at least 1, the result follows.  $\square$

**Lemma 6.8.** *In the subspace lattice, every vertical edge from  $S_i S_j$  to  $S_{i+1} S_j$  has weight 1 for  $i \geq 2$ .*

*Proof.* If not, then such an edge has weight 2, which implies that every edge on the sublattice of directed paths from  $S_1^2$  to  $S_i S_j$  has weight 1 by Lemma 6.7. But then Lemma 4.2 implies that  $S_j$  has a basis in geometric progression, which in turn implies that  $\dim S_j^2 = 2 \dim S_j - 1$ , meaning that all edges on the sublattice of paths from  $S_1^2$  to  $S_j^2$  have weight 1, a contradiction.  $\square$

Since any path from  $S_1^2$  to  $S_n^2$  has exactly one edge of weight 2 (Lemma 6.7), Lemma 6.8 implies that all horizontal edges  $S_i S_j \rightarrow S_i S_{j+1}$  of weight 2 occur for a common index  $j$ , that we call the *P-index* of the space  $S$ . Summarising:

**Lemma 6.9.** *There is an index  $j_0$ , called the P-index of  $S$ , such that  $\dim(S_i S_{j_0+1}) - \dim(S_i S_{j_0}) = 2$  for every  $i = 2 \dots j_0$ .*

The above proposition is illustrated on Figure 2.

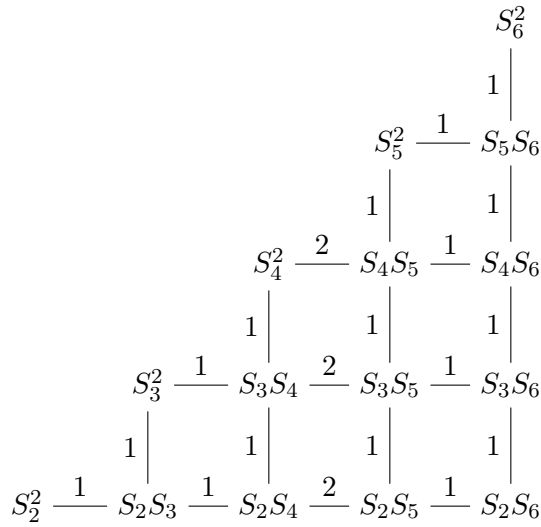


Figure 2:  $n = 6$  and  $j_0 = 4$  for the *P-index*

We will see later that there are only two possible values for the *P-index*, namely  $j_0 = 2$  and  $j_0 = n - 1$ .

## 6.5 Changing the valuation

A single valuation  $v_P$  may not be enough to describe sufficiently the spaces  $S_i$ , and it will be useful to involve alternative valuations. We now argue that some information obtained from a valuation  $v_P$  may be “transferred” and hence provide some information with respect to another valuation  $v_Q$ . When all weights are equal to 1 on the sublattice from  $S_i S_j$  to  $S_{i+1} S_{j+1}$ , i.e. in the situation illustrated on Figure 3, we have already observed (Lemma 4.1) that  $S_i S_{j+1} = S_{i+1} S_j$ .

From this equality, we conclude that for any place  $Q$ , we have  $v_Q(S_i S_{j+1}) = v_Q(S_{i+1} S_j)$ , and hence, thanks to Lemma 6.1,

$$- \min v_Q(S_{j+1}) + \min v_Q(S_j) = - \min v_Q(S_{i+1}) + \min v_Q(S_i). \quad (3)$$

Applying (3) when  $i = 2$  yields the following useful Lemma.

**Lemma 6.10.** *For every  $j \geq 2$  that differs from the P-index  $j_0$  of  $S$ , we have  $D_{S_{j+1}} - D_{S_j} = D_{S_3} - D_{S_2}$ .*

We now turn to determining the genus of  $F$ .

$$\begin{array}{ccc}
S_{i+1}S_j & \xrightarrow{1} & S_{i+1}S_{j+1} \\
\left| \begin{array}{c} 1 \\ \hline \end{array} \right. & & \left| \begin{array}{c} 1 \\ \hline \end{array} \right. \\
S_iS_j & \xrightarrow{1} & S_iS_{j+1}
\end{array}$$

Figure 3: weights are equal to 1

## 6.6 The genus of the ambient field

We prove first that  $F = K(S)$  is in fact generated by the subspace  $S_3$ .

**Lemma 6.11.** *We have  $F = K(S_3)$ .*

*Proof.* For any  $i \geq 1$ , we have

$$S_{i-1}S_i = S_{i-1}^2 + S_{i-1}e_i.$$

Lemma 6.7 asserts  $\dim(S_iS_{i-1}) - \dim S_{i-1}^2 \leq 2$ . Moreover, if  $i \geq 4$ ,  $\dim S_{i-1} \geq 3$  and hence the intersection  $S_{i-1}^2 \cap S_{i-1}e_i$  is non-zero. Consequently,  $e_i \in K(S_{i-1})$ . Therefore  $F = K(S_n) = K(S_{n-1}) = \cdots = K(S_3)$ .  $\square$

Remembering that  $e_1 = 1$ , and that we use the notation  $x = e_2$  and  $y = e_3$ , Lemma 6.11 says that  $F = K(x, y)$ . Our next goal will be to determine the genus of  $F$  and for this we will identify an equation of lowest degree satisfied by  $x$  and  $y$ : its degree will determine the genus of  $F$ .

**Proposition 6.12.** *The field  $F$  has genus less than or equal to 1.*

*Proof.* Depending on the value of the  $P$ -index being greater than 2 or equal to 2, we have either  $\dim S_2S_3 = 4$  or  $\dim S_2S_3 = 5$ . Moreover,  $S_2S_3$  is generated by  $(1, x, x^2, xy, y)$ .

If  $\dim S_2S_3 = 4$  then we get a linear relation between  $1, x, x^2, xy, y$  which immediately shows that  $y \in K(x)$  and consequently that  $F = K(x)$  and has genus 0. We note that we have found an irreducible quadratic relation between  $x$  and  $y$ , meaning that  $F$  is the function field of a plane irreducible conic.

If  $\dim S_2S_3 = 5$ , then  $1, x, x^2, xy, y$  are linearly independent over  $K$ ; the subspace  $S_3^2$ , which is generated by  $(1, x, y, x^2, xy, y^2)$  and has dimension 6, does also not produce an algebraic relation between  $x$  and  $y$ . We need to go to  $S_3S_4$ , which is of dimension 7 and is generated by  $(1, x, y, e_4, x^2, xy, xe_4, y^2, ye_4)$ . It entails the existence of two independent relations

$$e_4L_1(x, y) = Q_1(x, y) \tag{4}$$

$$e_4L_2(x, y) = Q_2(x, y) \tag{5}$$

where  $L_1, L_2$  are linear polynomials and  $Q_1, Q_2$  are quadratic polynomials. Moreover, the linear polynomials  $L_1, L_2$  are nonzero since  $\dim S_3^2 = 6$  and hence, there is no quadratic polynomial vanishing on  $x, y$ . By eliminating  $e_4$  we get

$$L_1(x, y)Q_2(x, y) = L_2(x, y)Q_1(x, y). \tag{6}$$

The polynomial  $L_1Q_2 - L_2Q_1$  is nonzero because the relations (4) and (5) are independent. This polynomial has degree at most 3 and, since  $\dim S_3^2 = 6$ , there is no quadratic relation

relating  $e_1, x, y$ , which asserts that the degree is exactly 3. Therefore, the genus of  $F$  is either 0 (if the curve of equation  $L_1Q_2 - L_2Q_1$  has a singularity) or 1, as a consequence of Bézout's Theorem [7].  $\square$

**Summary.** Writing  $S_2 = \langle 1, x \rangle$  and  $S_3 = \langle 1, x, y \rangle$ , we may distinguish three cases.

- (1)  $\dim S_2S_3 = 4$ . In this situation,  $F = K(x)$  and there is an irreducible quadratic polynomial  $Q$  such that  $Q(x, y) = 0$ .
- (2)  $\dim S_2S_3 = 5$  and there is a cubic relation  $L_1(x, y)Q_2(x, y) - L_2(x, y)Q_1(x, y) = 0$  such that the corresponding projective plane curve is singular.
- (3)  $\dim S_2S_3 = 5$  and there is a cubic relation  $L_1(x, y)Q_2(x, y) - L_2(x, y)Q_1(x, y) = 0$  such that the corresponding projective plane curve is smooth.

Cases (1) and (2) correspond to the genus 0 case. Case (3) correspond to the genus 1 case.

In order to finish the proof of Theorem 5.3, it remains to compute the divisor  $D_S$ , as defined in 6.2. For this, we will first determine  $D_{S_2}$  and  $D_{S_3}$ , and then, iteratively compute  $D_{S_i}$  for  $i \leq n$ .

## 6.7 The $P$ -index is equal to 2

In this subsection, we treat the case of the  $P$ -index being equal to 2, which amounts to  $\dim S_2S_3 = 5$ . We have already proved that  $x$  and  $y$  satisfy an equation of degree 3; in the next Lemma we show that moreover this equation has a specific form.

**Lemma 6.13.** *The field  $F = K(x, y)$  has degree 2 over  $K(x)$  and the equation satisfied by  $x$  and  $y$  is of the form*

$$y^2 + B(x)y + C(x) = 0 \tag{7}$$

where  $\deg B \leq 2$  and  $\deg C \leq 3$ .

*Proof.* The field  $F$  is generated by  $x$  and  $y$  and the proof of Proposition 6.12 has shown that there is a relation  $G(x, y) = 0$  of degree 3. Suppose that  $G(x, y)$  contains a term in  $y^3$  and write  $G(x, y)$  as

$$G(x, y) = y^3 + A(x)y^2 + B(x)y + C(x) = 0$$

where  $\deg A \leq 1$ ,  $\deg B \leq 2$  and  $\deg C \leq 3$ . By construction, we have  $v_P(y^3) < v_P(xy^2) < v_P(x^2y) < v_P(x^3)$  so  $v_P(y^3) < v_P(A(x)y^2 + B(x)y + C(x))$  which is in contradiction with  $G(x, y) = 0$ . So the equation has the form  $A(x)y^2 + B(x)y + C(x) = 0$ . With a similar reasoning we can see that moreover  $A(x)$  must be a constant. It remains to rule out the case when  $A(x) = 0$ , which would mean that  $y \in K(x)$  and  $F = K(x)$ . Let us assume we are in this case and reach a contradiction. Because  $v_P(x) < 0$ ,  $P = P_\infty$  is the place at infinity of  $K(x)$  and  $v_P(x) = -1$ . In particular  $D_{S_2} = L(P)$ . Regarding  $y$ , we know that  $v_P(y) < v_P(x)$  so the only possibility is  $v_P(y) = -2$  because of the structure of  $v_P(S)$  which contains  $\{0, -1\}$ : indeed, recall from Proposition 5.2 that it can have a missing element only after its first or before its last value and since  $n \geq 4$  the smallest value of  $v_P(S)$  is not  $v_P(y)$ . According to Lemma 6.5,  $S_2$  separates  $P$  and any other place  $Q \neq P$ ; according to Lemma 6.6, so does  $S_2S_4$ . But  $S_2S_4 = S_3^2$  from Lemma 4.1 which entails that also  $S_3$  separates  $P$  and  $Q$ . So  $y$  cannot have a pole at  $Q$ , which leaves the only possibility  $y = C(x)$  with  $\deg(C) = 2$ . But this situation is not compatible with the condition that  $\dim S_2S_3 = 5$ .  $\square$

**Proposition 6.14.** *When  $\dim S_2S_3 = 5$ , there is a place  $Q$ , possibly equal to  $P$ , such that, for all  $i = 2, \dots, n$ ,*

$$D_{S_i} = (i - 1)P + Q.$$

*Proof.* We first focus on determining the divisors of  $S_2$  and  $S_3$ . Because  $v_P(x) < 0$ , the place  $P$  is above the place at infinity of  $K(x)$ , that we will denote  $P_\infty$ . Since  $K(x, y)$  has degree 2 over  $K(x)$  by Lemma 6.13, we have from [13, Ch.3] that  $P_\infty$  decomposes in  $F = K(x, y)$  either as  $2P$  (the ramified case) or as  $P + Q$  where  $Q \neq P$  (the split case). For any other place  $R \notin \{P, Q\}$ , the valuation  $v_R(x)$  is non negative, and we have therefore  $D_{S_2} = 2P$  in the ramified case and  $D_{S_2} = P + Q$  in the split case. We now focus on determining  $D_{S_3}$ . From (7) the valuation  $v_R(y)$  can only be non negative for any place  $R \notin \{P, Q\}$ , so we are left with determining the valuation at  $P$  and  $Q$  of  $y$ .

We now view  $K(x, y)$  as an algebraic extension of  $K(y)$  instead of an extension of  $K(x)$ . We remark that  $P$ , respectively  $P$  and  $Q$  in the split case, are also the places above the place at infinity of  $K(y)$ . So, since  $[K(x, y) : K(y)] \leq 3$ , we also know from [13, Ch. 3] that  $v_P(y) \geq -3$ , and, in the split case, that  $v_P(y) + v_Q(y) \geq -3$ . Taking account of this, we see that in the ramified case  $2P$  we necessarily have  $v_P(x) = -2$  and  $v_P(y) = -3$ , and so,  $D_{S_2} = 2P$  and  $D_{S_3} = 3P$ .

In the split case  $P + Q$ , i.e.  $v_P(x) = v_Q(x) = -1$ , we can conclude so far that  $v_P(y) = -2$  or  $-3$ . But the case  $v_P(y) = -3$  would create a forbidden hole in  $v_P(S)$  that contains  $\{v_P(1) = 0, v_P(x) = -1\}$  (because not in first or last position). So the only possibility is  $v_P(y) = -2$ . Now since  $v_P(y) + v_Q(y) \geq -3$  we must have  $v_Q(y) \geq -1$ . So  $D_{S_2} = P + Q$  and  $D_{S_3} = 2P + Q$ .

Finally, to obtain  $D_{S_i} = (i - 1)P + Q$  for  $i \geq 4$  we apply Lemma 6.10.  $\square$

In the case when  $\dim S_2S_3 = 5$ , the above proposition concludes the proof of Theorem 5.3. Indeed, in the case when  $F$  is of genus 1, Riemann-Roch theorem tells us that  $S$  must coincide with the space  $L((n - 1)P + Q)$ . In the genus 0 case,  $S$  is of codimension 1 inside  $L((n - 1)P + Q)$ .

## 6.8 The $P$ -index is greater than 2, or the plane conic case

If  $S_2S_3$  has dimension 4, then recall that  $F = K(x)$  and that Lemma 4.2 implies that  $S_i$  is generated by  $(1, x, \dots, x^{i-1})$  for every  $i$ ,  $2 \leq i \leq k$ , where  $k$  is the  $P$ -index of  $S$ ; in other words, in this range,  $S_i = L((i - 1)P)$  where  $P = P_\infty$  is the place at infinity of  $K(x)$ .

**Lemma 6.15.** *We have  $D_{S_{k+1}} = kP + Q$  for some place  $Q$  possibly equal to  $P$ .*

*Proof.* Let  $z$  be such that  $S_{k+1} = S_k + Kz$  with  $z$  of minimum  $P$ -valuation in  $S_{k+1}$ . We already know that  $v_P(S_{k+1})$  is either an arithmetic progression or an arithmetic progression with a missing element, in other words either  $v_P(z) = -k$  or  $v_P(z) = -(k + 1)$ .

Consider first the case  $v_P(z) = -(k + 1)$ . Consider the product  $S_3S_{k+1}$  which must be of dimension  $(k + 1) + 3$ . The space  $S_3$  is generated by  $1, x, x^2$  and we have  $v_P(S_3S_{k+1}) \supset \{v_P(x^k), v_P(z), v_P(xz), v_P(x^2z)\}$  so that

$$v_P(S_3S_{k+1}) = \{0, -1, -2, \dots, -(k - 1), -k, -(k + 1), -(k + 2), -(k + 3)\}.$$

Since  $x^k = xx^{k-1}$  and  $x^{k+1} = x^2x^{k-1}$  are in  $S_3S_{k+1}$ , we have that  $S_3S_{k+1}$  contains the subspace generated by the geometric progression  $1, x, x^2, \dots, x^{k+1}$ , which is equal to the subspace of  $S_3S_{k+1}$  of functions of  $P$ -valuation  $\geq -(k + 1)$ , because this must be a space of dimension  $k + 2 = \dim S_3S_{k+1} - 2$ . Since  $v_P(z) = -(k + 1)$ , the function  $z$  must belong

to the aforementioned subspace, meaning that  $z$  is a polynomial in  $x$  of degree  $k + 1$ , in other words  $S_{k+1} \subset L((k + 1)P)$ .

Consider now the remaining case  $v_P(z) = -k$ . The set  $v_P(S_{k+1})$  is now the arithmetic progression  $\{0, -1, \dots, -k\}$  and we have  $D_{S_{k+1}} = kP + D$  for some positive divisor  $D$ . Consider again the product  $S_3S_{k+1}$  and let  $U$  be the subspace of those elements of  $S_3S_{k+1}$  that have a valuation greater than the minimum, namely  $-k - 2 = v_P(z) + v_P(x^2)$ . We have that  $U$  has codimension 1 in  $S_3S_{k+1}$  (Proposition 2.1) i.e.,  $\dim U = k + 3$ . Note also that  $U$  contains  $1, x, \dots, x^{k+1}$ , so that there exists  $u \in U$  of positive  $P$ -valuation, such that  $u, 1, x, \dots, x^{k+1}$  is a basis of  $U$ . Now since  $v_P(z) = -k$ , we have  $z \in U$  and

$$z = P_{k+1}(x) + \lambda u, \quad \lambda \in K \quad (8)$$

with  $P_{k+1}(x)$  a polynomial in  $x$  of degree at most  $k + 1$ . Note that we must have  $\lambda \neq 0$  otherwise, since  $v_P(z) = -k$ ,  $z$  is a polynomial of degree  $k$  in  $x$  contradicting that  $\dim S_3S_{k+1} = k + 4$ . The equality (8) implies therefore that  $\alpha \in K$  is a pole of  $z$  if and only if it is a pole of  $u$ . For such a pole  $\alpha$ , we have  $(x - \alpha)z \in U$  since  $v_P((x - \alpha)z) = -(k + 1)$ , hence

$$(x - \alpha)z = Q_{k+1}(x) + \mu u, \quad \mu \in K$$

for  $Q_{k+1}(x)$  a polynomial in  $x$  of degree at most  $k + 1$ . This implies that  $\mu = 0$  otherwise the left hand side and the right hand side would not have the same  $\alpha$ -valuation. This proves that  $z$  has a pole of order 1 at  $\alpha$  and simultaneously that  $z$  cannot have a pole at  $\beta$  for  $\beta \neq \alpha$ . Therefore  $z$  has a single pole of order 1 besides  $P_\infty$ .  $\square$

We conclude with the following statement.

**Proposition 6.16.** *The  $P$ -index  $k$  of  $S$  equals  $n - 1$ .*

*Proof.* In the case when  $Q = P$  in Lemma 6.15, since the set of  $P$ -valuations can only be an arithmetic progression with a hole in the last position, we must have  $k = n - 1$ . We may therefore suppose that  $Q \neq P$ .

Suppose towards a contradiction that  $k \leq n - 2$ . The space  $S_k$  is a Riemann-Roch space. Hence, from Lemma 6.5,  $S_k$  separates  $P$  with any place  $Q \neq P$  of  $F$ . Therefore, from Lemma 6.6 so does  $S_kS_{k+2}$ . On the other hand  $S_{k+1}$  does not separate  $P$  and  $Q$  and hence, again applying Lemma 6.6,  $S_{k+1}^2$  does not separate them either. This is a contradiction since, from Lemma 6.10,  $S_kS_{k+2}$  should be equal to  $S_{k-1}^2$ .  $\square$

As a conclusion, in this situation,  $S$  is a subspace of codimension 1 of a Riemann-Roch space of the form  $L((n - 1)P + Q)$  where  $Q$  is a place, possibly equal to  $P$ .

## 7 Further description of spaces with genus 0 and combinatorial genus 1

Theorem 5.3 gives a complete characterisation of spaces  $S$  of genus 1 with combinatorial genus  $\gamma = 1$  by saying that they are exactly Riemann-Roch spaces. However, in the case when the genus of the field  $F$  is 0, it only says that  $\gamma = 1$  implies that  $S$  is of codimension 1 inside a Riemann-Roch space: but not all subspaces of codimension 1 inside an  $L(D)$  space have combinatorial genus 1, so this raises the question of exactly which subspaces have  $\gamma = 1$ . The following theorem gives a precise answer.

**Theorem 7.1.** *Let  $S$  be of genus  $g = 0$  and of combinatorial genus  $\gamma = 1$ . Then, up to multiplication by a constant,  $S$  has a basis of one of the following two types:*

$$(i) \ 1, t, t^2, \dots, t^{n-2}, (t + \alpha)t^{n-1},$$

$$(ii) \ 1, (t + \alpha)t, (t + \alpha)t^2, \dots, (t + \alpha)t^{n-2}, (t + \alpha)t^{n-1}$$

for some function  $t$  and some constant  $\alpha \in K$ .

Before proving Theorem 7.1 we introduce an intermediate result. The proof of Theorem 5.3 has shown that  $S$  (after replacing it by a suitable multiplicative translate  $s^{-1}S$ ) is such that  $1 \in S$  and  $S \subset L((n-1)P+Q)$  where  $P$  is the initial arbitrary place of  $F = K(S)$  and  $Q$  is some place that may or may not be equal to  $P$ . The following proposition states that there always is a choice of  $P$  for which we have  $Q = P$ .

**Proposition 7.2.** *There exists a place  $P$  and a function  $s \in S$  such that  $s^{-1}S \subset L(nP)$ .*

*Proof.* We start with an arbitrary choice of  $P$  so that we may suppose  $1 \in S$  and  $S \subset L((n-1)P+Q)$  with  $Q \neq P$ . Since the action of  $\text{PGL}(2, K)$  on places is 3-transitive, we may choose a function  $t$  for which  $F = K(t)$  and such that  $P$  and  $Q$ , viewed over  $K(t)$ , are the place at infinity and the place at zero respectively. In other words  $L((n-1)P+Q)$  is the space of Laurent polynomials of the form

$$f(t) = \frac{a_{-1}}{t} + a_0 + a_1t + a_2t^2 + \dots + a_{n-1}t^{n-1} \quad (9)$$

Since  $S$  has codimension 1 inside  $L((n-1)P+Q)$ , there exist coefficients  $\lambda_{-1}, \lambda_0, \dots, \lambda_{n-1} \in K$ , such that  $S$  consists of the space of functions (9) satisfying

$$\lambda_{-1}a_{-1} + \lambda_0a_0 + \dots + \lambda_{n-1}a_{n-1} = 0. \quad (10)$$

If  $\lambda_{-1} = 0$  then  $\frac{1}{t} \in S$  so that  $1 \in tS$  and  $tS \subset L(nP)$  and we are finished. Suppose therefore  $\lambda_{-1} \neq 0$ . We claim there exists  $a \in K$  such that the function  $(t-a)^n \in tS$ . Indeed, expanding the expression  $(t-a)^n$  as

$$(t-a)^n = a_{-1} + a_0t + \dots + a_{n-1}t^n$$

we see that the quantity  $\lambda_{-1}a_{-1} + \dots + \lambda_{n-1}a_{n-1}$  is a polynomial in  $a$  of degree exactly  $n$ , which has roots in  $K$  since  $K$  is algebraically closed. For such an  $a$  we get that (10) is satisfied. Now since  $tS$  consists only of polynomials in  $t$ , equivalently in  $t-a$ , we have that the space  $\frac{1}{(t-a)^n}tS$  contains 1 and is included in  $L(nP_a)$  where  $P_a$  is the place at  $a$ .  $\square$

*Proof of Theorem 7.1.* Applying Proposition 7.2, we may suppose  $1 \in S \subset L(nP)$  and, without loss of generality, that  $P$  is the place at infinity over  $K(t)$ : in other words,  $S$  consists of a space of polynomials, of degree at most  $n$ , and including constants. The space  $S$  must contain a polynomial of degree  $n$ , otherwise, because  $\dim S = n$ ,  $S$  would be equal to the space  $L((n-1)P)$  and we would have  $\dim S^2 = 2 \dim S - 1$ , contradicting  $\gamma = 1$ . Since  $S$  contains constants we have that the set of degrees  $d(S)$  of the elements of  $S$  is included in the arithmetic progression  $\{0, 1, \dots, n\}$ , and since we may find at most  $2n$  different degrees in  $S^2$ , Proposition 5.2 implies that

1. either  $d(S) = \{0, 1, 2, \dots, n-3, n-2, n\}$ ,
2. or  $d(S) = \{0, 2, 3, \dots, n-2, n-1, n\}$ .



In case 1, we have that  $S$  contains as a subspace the space of all polynomials of degree at most  $n - 2$ , and also a polynomial of degree  $n$ . This gives the existence of the basis of type (i) mentioned by the Theorem. It remains to deal with case 2 for which there exists a basis of  $S$  of the form

$$1, p_2, p_3, \dots, p_n$$

where  $p_i$  is a polynomial of degree  $i$  in the variable  $t$ . Consider the sequence of subspaces

$$S_1 = K \subset S_2 \subset \dots \subset S_n = S$$

where  $S_i = S_{i-1} + Kp_i$  for  $i \geq 2$ . We shall prove by induction on  $k$  that for  $k = 3, 4, \dots, n$ , the space  $S_k$  has, possibly after changing the variable  $t$ , a basis of the form  $1, (t + \alpha)t, \dots, (t + \alpha)t^{k-1}$ , yielding the desired basis of  $S$  for  $k = n$ . Write the Euclidean division of  $p_3$  by  $p_2$ ,

$$p_3 = (t + a)p_2 + bt + c$$

where we have set the leading coefficients of  $p_2$  and  $p_3$  equal to 1. By replacing if need be  $p_2$  by  $p_2 + b$  and  $p_3$  by  $p_3 + ab - c$  we see that we may suppose that  $p_2$  divides  $p_3$ . Without loss of generality (change the variable  $t$  to  $t - \beta$ ,  $\beta \in K$ ), we may suppose that one of the roots of  $p_2$  is 0, so that  $p_2 = (t + \alpha)t$  for some constant  $\alpha$ , and we have that  $S_3$  has a basis of the required form, possibly after adding to  $p_3$  a scalar multiple of  $p_2$ .

Suppose now that  $S_k$  has a basis of the required form,  $3 \leq k \leq n - 1$ , and consider  $S_{k+1} = S_k + Kp_{k+1}$ . Without loss of generality suppose  $p_{k+1}$  has no constant term, i.e. is divisible by  $t$  (replacing  $p_{k+1}$  by  $p_{k+1} + c$ ,  $c \in K$ , does not change the space  $S_{k+1}$ ). Let  $T_k$  be the subspace of  $S^2$  consisting of all polynomials in  $t$  of degree at most  $k + 1$ . Now the set of degrees of  $S^2$  is  $0, 2, 3, \dots, 2n$ , which implies that  $T_k$  cannot be equal to the whole space of polynomials of degree at most  $k + 1$  so that  $\dim T_k \leq k + 1$ . Notice also that  $T_k$  contains

$$1, (t + \alpha)t, (t + \alpha)t^2, \dots, (t + \alpha)t^{k-1} \quad (11)$$

which are all in  $S_k$  by the induction hypothesis, and  $T_k$  contains also

$$(t + \alpha)^2 t^{k-1} = (t + \alpha)t \times (t + \alpha)t^{k-2}.$$

Since  $\dim T_k \leq k + 1$ , a basis of  $T_k$  is therefore given by (11) together with  $(t + \alpha)^2 t^{k-1}$ . Now  $p_{k+1} \in T_k$ , so that it decomposes over the above basis, and since  $p_{k+1}$  has no constant term, we have just proved that it is a multiple of  $(t + \alpha)t$ , which shows the existence of a basis of  $S_{k+1}$  of the required form.  $\square$

Theorem 7.1 shows in particular that there always exists a valuation  $v$ , for which the set of valuations  $v(S)$  of a space of genus 0 and combinatorial genus 1 is an arithmetic progression with a missing element (after the first or last position). In contrast, the set of valuations for an arbitrary  $v$  will typically be an arithmetic progression. We now make the remark that when  $g = 1$  and  $\gamma = 1$ , there also always exists a valuation  $v$  for which  $v(S)$  is an arithmetic progression with a missing element.

Denote by  $\sim$  the linear equivalence of divisors, and recall that  $G \sim H$  means that  $L(G) = fL(H)$  for some function  $f$ .

**Lemma 7.3.** *Let  $E$  be an elliptic curve and  $G$  be a divisor on  $E$  of degree  $d$ . Then, there exists a point  $R$  of  $E$  such that  $G \sim dR$ .*

*Proof.* Let  $G = r_1P_1 + \dots + r_sP_s$ . Denote by  $\oplus$  the group law on the elliptic curve. Let  $P = r_1P_1 \oplus \dots \oplus r_sP_s$ . From [12, Proposition III.3.4], we get  $G - dO \sim P - O$  where  $O$  is the zero element of the group of points of  $E$ .

Over an algebraically closed field the group of points of  $E$  is divisible (see [12, Theorem 4.10(a)]), hence there exists  $R \in E$  such that  $Q = dR$ . Therefore:

$$G - dO \sim d(R - O) \implies G \sim dR.$$

□

*Remark 7.4.* According to the proof, the point  $R$  may be non unique since it can be replaced by the point  $R \oplus T$  where  $T$  is a  $d$ -torsion point. Thus, if  $d$  is prime to the characteristic of  $K$  there are  $d^2$  possibilities for  $R$ .

Consequently,  $S$  is of the form  $fL(nR)$  for some place  $R$  and some nonzero function  $f$ . It is well-known that the sequence of valuations of a space  $L(nR)$  is  $\{0, -2, -3, \dots, -n\}$ , which can be easily derived from the Riemann-Roch Theorem. Multiplication by  $f$  only translates the sequence of valuations.

## Acknowledgements

The authors are supported by French *Agence nationale de la recherche* grant ANR-15-CE39-0013-01 *Manta*.

## References

- [1] C. Bachoc, O. Serra and G. Zémor. An analogue of Vosper’s Theorem for Extension Fields, *Math. Proc. Cambridge Philos. Soc.*, to appear
- [2] C. Bachoc, O. Serra and G. Zémor Revisiting Kneser’s Theorem for Field Extensions, *Combinatorica*, to appear.
- [3] V. Beck and C. Lecouvey, Additive combinatorics methods in associative algebras, preprint (2015) <http://arxiv.org/abs/1504.02287>
- [4] N. Bourbaki. *Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations.* Actualités Scientifiques et Industrielles, No. 1308. Hermann, Paris, 1964.
- [5] S. Eliahou and C. Lecouvey, On linear versions of some addition theorems. *Linear Multilinear A.* 57, 759–775 (2009).
- [6] G. Freiman. *Foundations of a structural theory of set addition*, volume 37 of *Mathematical Monograph*. Amer. Math. Soc., 1973.
- [7] W. Fulton. *Algebraic curves.* Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.
- [8] M. Kneser. Summenmengen in lokalkompakten abelsche Gruppen. *Math. Z.* 66 (1956), 88–110.
- [9] X. Hou, K.H. Leung, and Q. Xiang. A generalization of an addition theorem of Kneser. *J. Number Theory.* 97 (2002), 1–9.

- [10] D. Mirandola and G. Zémor. Critical pairs for the Product Singleton Bound, *IEEE Trans. on Information Theory*, IT-61, No 9 (2015) pp. 4928– 4937.
- [11] D. Mumford. Varieties defined by quadratic equations. In *Questions on algebraic varieties, C.I.M.E., III Ciclo, Varenna, 1969*, pages 29–100. Edizioni Cremonese, Rome, 1970.
- [12] J. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2009.
- [13] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
- [14] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2006.
- [15] G. Vosper. The critical pairs of subsets of a group of prime order. *J. London Math. Soc.* 31 (1956), 200–205.