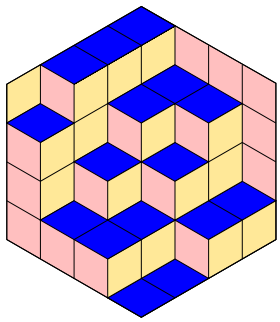


ALGEBRAIC COMBINATORICS

Christine Bachoc, Alain Couvreur & Gilles Zémor

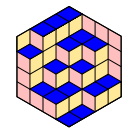
Towards a function field version of Freiman's Theorem

Volume 1, issue 4 (2018), p. 501-521.

<http://alco.centre-mersenne.org/item/ALCO_2018___1_4_501_0>

Algebraic Combinatorics is member of the
Centre Mersenne for Open Scientific Publishing
www.centre-mersenne.org

Algebraic Combinatorics
Volume 1, issue 4 (2018), p. 501–521
https://doi.org/10.5802/alco.19



Towards a function field version of Freiman's Theorem

Christine Bachoc, Alain Couvreur & Gilles Zémor

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 $\dim S^2 \leqslant 3\dim S - 4$. 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 [10]. 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, 11]. Linear versions of addition theorems were also studied in the somewhat broader context of skew field extensions in [5]. Many applications of the theory of products of spaces in the algebra $\mathbf{F}_q^n$ with componentwise multiplication are discussed in [13].

A common feature of many 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

Manuscript received 15th September 2017, revised 18th April 2018, accepted 7th May 2018.

Keywords. Additive combinatorics, function fields.

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

where there are no subextensions of K in F (K is algebraically closed in F) in which case one always has $\dim ST \geqslant \dim S + \dim T - 1$ whenever $ST \neq F$ [5]. The goal of [1] was to prove that the equality $\dim ST = \dim S + \dim T - 1$ essentially implies that S and T have bases in geometric progression: this is a linear equivalent of Vosper's Theorem [18] 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. This theory of subspaces with products of small dimension in field extensions has also recently found applications to coding theory in [14].

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 γ. 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], [17, Theorem 5.11], which says that in a torsion-free abelian group,

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

implies, when $\gamma \leqslant |A| - 3$, that A is included in an arithmetic progression of length $|A| + \gamma$ (i.e. A is a progression with at most γ missing elements). The full Freiman Theorem, which extends the above $3k-4$ version, is arguably a cornerstone of additive combinatorics and has inspired a lot of subsequent work (see e.g. [17]). In this light, tackling the characterisation of spaces satisfying (1) would be a welcome addition to the burgeoning theory of space products in extension fields.

Candidates for spaces S satisfying (1) are of course subspaces (of codimension at most γ) inside a space that has a basis in geometric progression. However, some thought yields alternative spaces that do not have an additive analogue when $\gamma \geqslant 1$: namely Riemann–Roch spaces $L(D)$ of an algebraic curve of genus γ, which can be 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) with $\gamma \leqslant \dim S - 3$ 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 $t + g \leqslant \gamma$. With this in mind, let us call the quantity γ 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 starts with a discussion of concrete examples of spaces with small products. Section 3 recalls basic properties of valuations that will in particular associate sets of integers with small sumsets to subspaces with products of small dimension. Section 4 proves Theorem 4.2, 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 5 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 6 recalls basic properties of Riemann–Roch spaces and states the paper's main result, Theorem 6.3.

Section 7 proves Theorem 6.3. Section 8 complements Theorem 6.3 by giving a precise characterisation of those subspaces of Riemann–Roch spaces that have combinatorial genus equal to 1. Finally, Section 9 extends Theorems 4.2 and 6.3 to the case when the base field is perfect rather than algebraically closed.

2. Motivating Examples

Let K be a field and consider the field $F = K(x)$ of rational functions over K. Suppose we want a K-vector subspace S of dimension k such that S^2 has the smallest possible dimension. A natural candidate is the space S generated by the geometric progression $1, x, x^2, \ldots, x^{k-1}$ for which we have $\dim S^2 = 2k-1$. We notice that the set A of degrees of the rational functions (in this example polynomials in x) of S is an arithmetic progression. More generally, the set of degrees of the functions in S^2 must contain $A + A$, so that $\dim S^2 \geqslant |A + A|$. This remark may be used to claim that if $\dim S^2$ is the smallest possible, namely $2k-1$, then $|A + A|$ must be as small as possible, which implies that A must be an arithmetic progression of integers, from which it is fairly straightforward to deduce that S must have a basis of elements in geometric progression. We will make the point below that this line of reasoning extends to other extension fields F of K, provided we have *valuations* at our disposal to generalise degrees of rational functions.

Next relax slightly the condition on $\dim S^2$ to $\dim S^2 \leqslant 2k$. To construct examples of such spaces we may consider S in the rational function field $K(x)$ generated by $1, x^2, x^3, \ldots, x^k$. These spaces are directly inspired from the sets of integers $A = \{0, 2, 3, \ldots, k\}$ such that $|A + A| = 2|A|$. However, we have additional examples of such spaces that have no direct additive counterpart: take K to be the field of complex numbers (say) and take F to be the algebraic extension $K(x, y)$ of the rational function field $K(x)$ where y satisfies the equation $y^2 - x^3 + x = 0$. Now consider the space S of dimension 5 generated by $1, x, y, x^2, xy$. It is readily checked that we have $\dim S^2 = 2 \dim S$. The space S is an example of a Riemann–Roch space of the algebraic curve of equation $y^2 - x^3 + x = 0$ which is elliptic or of genus 1. Our main result, namely Theorem 6.3, will tell us that these two examples are in some sense generic. This has motivated the following definition, and also the conjecture below:

Definition 2.1. *Let K be a field and F be a K–algebra. Let $S \subset F$ be a finite dimensional K–subspace of F. The* combinatorial genus of S *is defined as the integer γ such that*

$$\dim S^2 = 2 \dim S - 1 + \gamma.$$

Conjecture 2.2. *Let K be an algebraically closed field and let F be an extension field of K. Let S be a K-subspace of finite dimension in F such that $K \subset S$. Let the combinatorial genus γ of S satisfy $\gamma \leqslant \dim S - 3$. Then the genus g of the field $K(S)$ satisfies $g \leqslant \gamma$ and there exists a Riemann–Roch space $L(D)$ that contains S and such that $\dim L(D) \leqslant \dim S + \gamma - g$.*

The next section recalls some background on valuations with which we will derive our first results on spaces with small combinatorial genus.

3. Function fields, 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. We refer the reader to [4, Chapter 6] for further details.

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 functions 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, $v(x+y) \geqslant \min\{v(x), v(y)\}$ with equality when $v(x) \neq v(y)$. The map v is extended to F with the convention $v(0) = \infty$.

A valuation comes with *a valuation ring* $\mathcal{O} \subset F$ which is defined as the set of functions of non-negative valuation, together with addition and multiplication inherited from F. A valuation ring has a unique maximal ideal $\mathfrak{m}$ equal to the set of elements of positive valuation. The quotient $\mathcal{O}/\mathfrak{m}$ is called the *residue field* of the valuation ring.

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 3.1. *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*

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

Such a basis is referred to as a filtered basis*. In addition, S has a natural filtration*

$$\{0\} \subset S_1 \subset \cdots \subset S_{n-1} \subset S_n$$

such that

$$\min v(S_1) > \cdots > \min v(S_{n-1}) > \min v(S). \tag{2}$$

For every $i = 1, \dots, n$, the space S_i is generated by $e_1, \dots, e_i$, but the filtration is uniquely defined and does not depend on the choice of 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 $v(a_1x_1 + \cdots + a_kx_k) = \min(v(x_1), \dots, v(x_k))$ must be finite, meaning $a_1x_1 + \cdots + a_kx_k$ must be non-zero. This shows that $|v(S)| \leqslant \dim S$.

Now let E be a subspace of S such that $v(E) = v(S)$ and suppose $E \subsetneqq S$. Let x be an element of $S \smallsetminus E$ with maximal valuation in $\{v(s), s \in S \smallsetminus E\}$. 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 $xe^{-1} \equiv \lambda \mod \mathfrak{m}$. 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.

Finally, the filtration $S_1 \subset \cdots \subset S_n = S$ is iteratively constructed as follows,

$$S_{i-1} = \{x \in S_i \mid v(x) > \min v(S_i)\}.$$

Note that this definition is independent of the choice of a filtered basis, however one checks easily that S_{i-1} is spanned by $e_1, \dots, e_{i-1}$. This shows that the space S_{i-1} has codimension 1 in S_i and the sequence of inequalities (2) follows immediately from the definition of the S_i's. □

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 3.2. *For any valuation v on F, and any K–subspace S,*

$$v(S) + v(S) \subseteq v(S^2). \tag{3}$$

Remark 3.3. 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 $H^2 = \langle \frac{1}{x}, 1, x, x^2, \ldots, x^5, x^6+\frac{1}{x^2}\rangle$ whose valuation set contains $v(1/x) = 1$ which is not in $v(H) + v(H)$.

From now on and until the end of Section 8 (with a temporary exception in §6.1), we suppose that the base field K is algebraically closed. Note that this assumption entails that any valuation on F has residue field K, which will therefore enable us to apply Proposition 3.1. Only in Section 9 will we consider what becomes of our results when the base field K is not algebraically closed.

4. Transposing Freiman's Lemma in field extensions

Recall the following result of Freiman [6], named "Freiman's Lemma" by Tao and Vu [17, Lemma 5.13].

Theorem 4.1. *Let A be a finite subset of $\mathbf{R}^d$ such that no hyperplane of $\mathbf{R}^d$ contains a translate of A. Then*

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

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 6.3 in Section 6.2).

We have the extension field analogue of Theorem 4.1.

Theorem 4.2. *Let K be an algebraically closed field and let $F \supseteq K$ be an extension field of K. Let S be a K-vector subspace of F of finite dimension and of transcendence degree d. Then*

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

The proof of Theorem 4.2 rests upon the following lemma.

Lemma 4.3. *If F/K is a field extension over an algebraically closed field K, and if $x_1, \ldots, x_d$ are K-algebraically independent elements of F such that F is an algebraic extension of $K(x_1, \ldots, x_d)$, 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 $v(x_1), v(x_2), \ldots, v(x_d)$ generate a group isomorphic to $\mathbf{Z}^d$.*

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

Proof of Theorem 4.2. Without loss of generality we may suppose $K \subset S$ and $F = K(S)$.

Let $x_1, \ldots, x_d$ be d algebraically independent elements of F. Choose for v a valuation given by Lemma 4.3. Then, since the residue field associated to v is K, by Proposition 3.1 we know that $\dim S = |v(S)|$ and $\dim S^2 = |v(S^2)|$. From (3) we have $\dim S^2 \geqslant |v(S) + v(S)|$ and Theorem 4.1 now gives us

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

which proves the theorem. □

Consequence. When one considers a space S, $K \subset S \subset F$, with $\dim S^2 \leqslant 3 \dim S - 4$, and $F = K(S)$, then F is a function field in one variable. In particular, from [16, Theorem 1.1.16], every valuation on F is discrete and its set of values is $\mathbf{Z}$.

For the rest of this article we will assume this setting, namely a sufficiently small combinatorial genus γ, 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).

5. 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.

5.1. The lattice of subspaces. Let $(e_1, \ldots, e_n)$ be a filtered basis of the space S relative to a valuation v. Consider the sequence of subspaces introduced in Proposition 3.1

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

where S_i denotes the subspace of S generated by $e_1, \ldots, e_i$. We will refer to this sequence of spaces as the *filtration of S relative to v*.

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_iS_j and ordered by inclusion, as represented on Figure 1. We will consider directed edges between S_iS_j and S_iS_{j+1} and between S_iS_j and $S_{i+1}S_j$, and label both edges by a weight defined as the codimension of S_iS_j inside S_iS_{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_ie_{j+1} is an element of minimal valuation of S_iS_{j+1} that cannot belong to S_iS_j because the minimum of $v(S_iS_j)$ is attained by e_ie_j, and similarly for $S_{i+1}S_j$.

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 5.1. *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 $U \subsetneqq S_{i+1}S_{j+1}$ 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. □

5.2. 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 5.2. *Suppose all directed edges lying on any path from S_1 to S_iS_j, $2 \leqslant i$, have weight 1. Then for every k, $2 \leqslant k \leqslant j$, the space S_k is generated by $1, x, x^2, \ldots, x^{k-1}$.*

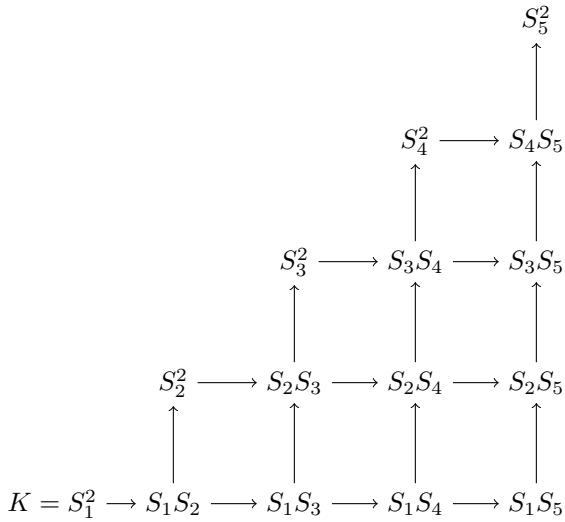


FIGURE 1. the lattice of subspaces

Proof. Proceed by induction on k. Suppose the result is proved for k and prove it for $k+1 \leqslant j$. By applying Lemma 5.1 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 $(1, x, x^2, \ldots, x^k)$. □

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 5.3. *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 $(a, ax, ax^2, \ldots, ax^{n-1})$.*

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 5.2. □

We now turn to Riemann–Roch spaces that provide more spaces of low combinatorial genus γ.

6. Divisors, Riemann–Roch spaces, and characterising spaces with combinatorial genus $\gamma = 1$

6.1. 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 [16] or to [7] for a more geometric point of view. In the present subsection, in order to introduce some notions that will also be useful in the more general setting of Section 9, we do not assume that K is algebraically closed.

Let F be a function field over K such that K is algebraically closed in F. Following [16, Chapter I], let us call a *place* P of F the maximal ideal of a valuation ring. Valuations, valuation rings, places are interchangeable notions in the sense that any one unambiguously defines the others. Informally, a place captures the concept of "point" of the associated algebraic curve. For a place P we denote by v_P the (unique)

associated discrete valuation. The *degree* $\deg P$ of a place P is the dimension over K of its residue field $\mathcal{O}/P$. It is always finite and equal to 1 when K is algebraically closed.

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

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

The group of divisors is partially ordered as follows: given a divisor $G = g_1P_1 + \cdots + g_mP_m$, we have $G \geqslant 0$ if $g_1, \ldots, g_m \geqslant 0$. Next $G \geqslant H$ if $G - H \geqslant 0$. The *degree* of the divisor G is defined as

$$\deg G = g_1 \deg P_1 + \cdots + g_m \deg P_m.$$

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

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

The dimension of this space is given by the famous Riemann–Roch theorem [16, 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 (see [16, Definition 1.4.15] for a definition).

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 $L(D) = f \cdot L(D')$.

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

Theorem 6.1 ([12, Theorem 6]). *Let D, D' be two divisors of a function field F of genus g over an algebraically closed field K. Suppose that* $\deg D \geqslant 2g$ *and* $\deg D' \geqslant 2g + 1$. *Then*

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

In particular, combining the Riemann–Roch theorem with Theorem 6.1, 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 $\gamma = g$. This has in particular motivated Definition 2.1.

Finally recall that, over an algebraically closed field K, 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 $1, x, x^2, \ldots, x^n$ is equal to the Riemann–Roch space $L(nP_\infty)$ where P_∞ is the place at infinity. We remark that the statement of Theorem 5.3 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.

6.2. Statement of the main theorem. Until the end of Section 8, the base field K is supposed to be algebraically closed.

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 4,

we know from Theorem 4.2 that the transcendence degree 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 6.2. *A subset A of the integers, $|A| \geqslant 4$, is such that $|A + A| = 2|A|$ if and only if it is of the form $A = a + \{0, 2d, 3d, \ldots, (n-1)d, nd\}$ for some integer a and 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. Proposition 6.2 is also true in the integers modulo a prime p, provided $|A + A| \leqslant p - 2$, see [8] (and is therefore necessarily true in $\mathbf{Z}$).

To generate a space S such that $\gamma = 1$, Proposition 6.2 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 6.1 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 cover all possible cases:

THEOREM 6.3. *Let K be an algebraically closed field and F be a function field over K. Let $S \subseteq F$, $1 \in S$, be a space of finite dimension $n \geqslant 4$ 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 γ equal to 1. For instance the space $S = \langle 1, x, x^3, x^4 \rangle$ has codimension 1 in a Riemann Roch space of a field of genus 0, while it has combinatorial genus 2. We postpone to Section 8 the precise characterisation of such subspaces which is slightly more involved than in the additive case given by Proposition 6.2.

7. Proof of Theorem 6.3

7.1. 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

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

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

Next we define (Section 7.2) the divisor D_U of a space U to be the smallest divisor such that the Riemann–Roch space $L(D_U)$ 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 $i \geqslant 2$.

We will consider closely the lattice of subspaces introduced in Section 5.1 and exploit the fact that most of its edges are of weight 1. A crucial intermediate result will be Lemma 7.10 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 7.3 and 7.4 build up material leading up to Section 7.5 which derives Lemma 7.10.

Section 7.6 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 $g \leqslant 1$. We then turn to determining the sequence (D_{S_i}) exactly. Lemma 7.10 tells us that when the P-index equals 2, the divisors D_{S_2} and D_{S_3} determine the whole sequence. In Section 7.7 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 $0, P + Q, 2P + Q, 3P + Q, \ldots, (n-1)P + Q$. Section 7.8 deals with the remaining case, for which it is shown that the sequence of divisors must be of the form $0, P, 2P, \ldots, (n-2)P, (n-1)P + Q$.

7.2. Minimum valuations, the divisor of a space. The following lemma is straightforward:

Lemma 7.1. *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 7.2. *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 $U \subseteq L(D)$.

7.3. Separation.

Definition 7.3 (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*

(1) $v_{P_i}(f_i) = \min v_{P_i}(U)$ *for* $i \in \{1, 2\}$;
(2) *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 7.4. *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 7.5. *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 7.4. □

The next lemma deals with separation in products of spaces.

LEMMA 7.6. *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

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

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. □

7.4. THE LATTICE OF SUBSPACES AND THE P-INDEX OF A SPACE. For the remainder of Section 7, P is a fixed arbitrary place of $F = K(S)$. We choose a filtered basis $(e_1, \ldots, e_n)$ where, having replaced S by $e_1^{-1}S$ if necessary, we have set $e_1 = 1$. We consider the filtration $S_1 \subset S_2 \subset \cdots \subset S_n = S$ associated to P, together with the lattice of subspaces $S_i S_j$ introduced in Section 5.1 and illustrated in Figure 1. Recall that the weight of an edge $V \to W$ is given by the codimension of V in W. In the case $\dim S^2 = 2 \dim S$ we have:

LEMMA 7.7. *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. □

LEMMA 7.8. *In the subspace lattice, every vertical edge from $S_i S_j$ to $S_{i+1} S_j$ has weight 1 for $i \geqslant 2$.*

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 7.7. But then, Lemma 5.2 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. □

Since any path from S_1^2 to S_n^2 has exactly one edge of weight 2 (Lemma 7.7), Lemma 7.8 implies that all horizontal edges $S_i S_j \to S_i S_{j+1}$ of weight 2 occur for a common index j, that we call the *P–index* of the space S. Summarising:

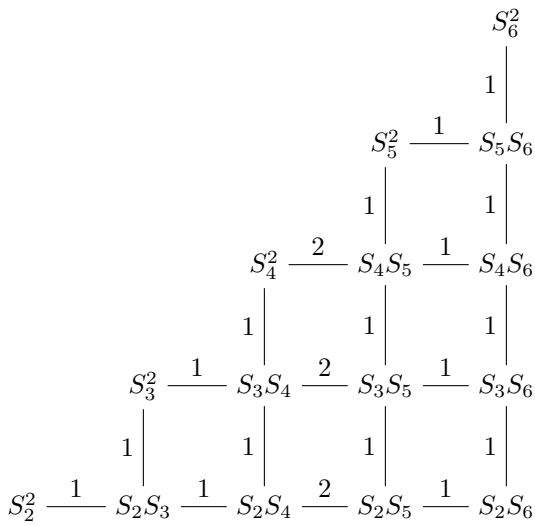


Figure 2. $n = 6$ and $j_0 = 4$ for the P-index

Lemma 7.9. *There is an index j_0, called the* P-index *of S, such that* $\dim(S_iS_{j_0+1}) - \dim(S_iS_{j_0}) = 2$ *for every $i = 2, \dots, j_0$.*

The above statement is illustrated on Figure 2.

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

7.5. 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_iS_j to $S_{i+1}S_{j+1}$, i.e. in the situation illustrated on Figure 3, we have already observed (Lemma 5.1) that

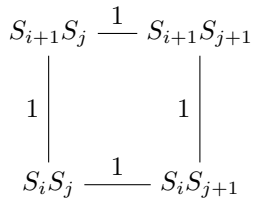


Figure 3. weights are equal to 1

$S_iS_{j+1} = S_{i+1}S_j$.

From this equality, we conclude that for any place Q, we have

$$v_Q(S_iS_{j+1}) = v_Q(S_{i+1}S_j),$$

and hence, thanks to Lemma 7.1,

$$-\min v_Q(S_{j+1}) + \min v_Q(S_j) = -\min v_Q(S_{i+1}) + \min v_Q(S_i). \tag{4}$$

Applying (4) when $i = 2$ yields the following useful lemma.

LEMMA 7.10. *For every $j \geqslant 2$ 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.

7.6. THE GENUS OF THE AMBIENT FIELD. We prove first that $F = K(S)$ is in fact generated by the subspace S_3.

LEMMA 7.11. *We have $F = K(S_3)$.*

Proof. For any $i \geqslant 1$, we have

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

Lemma 7.7 asserts $\dim(S_iS_{i-1}) - \dim S_{i-1}^2 \leqslant 2$. Moreover, if $i \geqslant 4$, $\dim S_{i-1} \geqslant 3$ 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 $F = K(S_n) = K(S_{n-1}) = \cdots = K(S_3)$. □

Remembering that $e_1 = 1$, and that we use the notation $x = e_2$ and $y = e_3$, Lemma 7.11 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 7.12. *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

$$e_4L_1(x, y) = Q_1(x, y) \tag{5}$$

$$e_4L_2(x, y) = Q_2(x, y) \tag{6}$$

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

$$L_1(x, y)Q_2(x, y) = L_2(x, y)Q_1(x, y). \tag{7}$$

The polynomial $L_1Q_2 - L_2Q_1$ is nonzero because the relations (5) and (6) 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]. □

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 6.3, it remains to compute the divisor D_S, as defined in 7.2. For this, we will first determine D_{S_2} and D_{S_3}, and then, iteratively compute D_{S_i} for $i \leqslant n$.

7.7. 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 7.13. *The field $F = K(x,y)$ has degree 2 over $K(x)$ and the equation satisfied by x and y is of the form*

$$y^2 + B(x)y + C(x) = 0 \tag{8}$$

where $\deg B \leqslant 2$ *and* $\deg C \leqslant 3$.

Proof. The field F is generated by x and y and the proof of Proposition 7.12 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 $\deg A \leqslant 1$, $\deg B \leqslant 2$ and $\deg C \leqslant 3$. 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 6.2 that it can have a missing element only after its first or before its last value and since $n \geqslant 4$ the value before the smallest value of $v_P(S)$ cannot be $v_P(y)$. According to Lemma 7.5, S_2 separates P and any other place $Q \neq P$; according to Lemma 7.6, so does S_2S_4. But $S_2S_4 = S_3^2$ from Lemma 5.1 which entails that also S_3 separates P and Q. So y cannot have a pole at Q, which leaves the only possibility $y = D(x)$ for some polynomial D with $\deg(D) = 2$. But this situation is not compatible with the condition that $\dim S_2S_3 = 5$. □

Proposition 7.14. *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_∞. Since $K(x,y)$ has degree 2 over $K(x)$ by Lemma 7.13, we have from [16, Chapter 3] that P_∞ 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 (8) 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 $[K(x,y) : K(y)] \leqslant 3$, we also know from [16, Chapter 3] that $v_P(y) \geqslant -3$, and, in the split case, that $v_P(y) + v_Q(y) \geqslant -3$. 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 $v_P(y) + v_Q(y) \geqslant -3$ we must have $v_Q(y) \geqslant -1$. So $D_{S_2} = P+Q$ and $D_{S_3} = 2P+Q$.

Finally, to obtain $D_{S_i} = (i-1)P + Q$ for $i \geqslant 4$ we apply Lemma 7.10. □

In the case when $\dim S_2S_3 = 5$, the above proposition concludes the proof of Theorem 6.3. 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 $L((n-1)P+Q)$.

7.8. 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 5.2 implies that S_i is generated by $(1, x, \ldots, x^{i-1})$ for every i, $2 \leqslant i \leqslant k$, 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 7.15. *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

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

Since $x^k = xx^{k-1}$ and $x^{k+1} = x^2x^{k-1}$ are contained in S_3S_{k+1}, we have that S_3S_{k+1} contains the subspace generated by the geometric progression $1, x, x^2, \ldots, x^{k+1}$, which is equal to the subspace of S_3S_{k+1} of functions of P-valuation $\geqslant -(k+1)$, 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 $\{0, -1, \ldots, -k\}$ 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 at P 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 3.1) i.e., $\dim U = k+3$. Note also that U contains $1, x, \ldots, x^{k+1}$, so that there exists $u \in U$ of positive P-valuation, such that $u, 1, x, \ldots, x^{k+1}$ is a basis of U. Now since $v_P(z) = -k$, we have $z \in U$ and

$$z = P_k(x) + \lambda u, \quad \lambda \in K \tag{9}$$

with $P_k(x)$ a polynomial in x of degree at most k. 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 (9) 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 α, 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 α-valuation. This proves that z has a pole of order 1 at α and simultaneously that z cannot have a pole at β for $\beta \neq \alpha$. Therefore z has a single pole of order 1 besides P_∞. □

We conclude with the following statement.

Proposition 7.16. *The P–index k of S equals $n-1$.*

Proof. In the case when $Q = P$ in Lemma 7.15, 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 $k \leqslant n-2$. The space S_k is a Riemann–Roch space. Hence, from Lemma 7.5, S_k separates P with any place $Q \neq P$ of F. Therefore, from Lemma 7.6 so does S_kS_{k+2}. On the other hand S_{k+1} does not separate P and Q and hence, again applying Lemma 7.6, S_{k+1}^2 does not separate them either. This is a contradiction since, from Lemma 7.10, S_kS_{k+2} should be equal to S_{k+1}^2. □

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.

8. Further description of spaces with genus 0 and combinatorial genus 1

Theorem 6.3 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 8.1. *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:*

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

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

Before proving Theorem 8.1 we introduce an intermediate result. The proof of Theorem 6.3 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 8.2. *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 $\mathrm{PGL}(2, K)$ 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

$$f(t) = \frac{a_{-1}}{t} + a_0 + a_1 t + a_2 t^2 + \cdots + a_{n-1} t^{n-1}. \tag{10}$$

Since S has codimension 1 inside $L((n-1)P + Q)$, there exist coefficients λ_{-1}, $\lambda_0, \ldots, \lambda_{n-1}$ in K, such that S consists of the space of functions (10) satisfying

$$\lambda_{-1} a_{-1} + \lambda_0 a_0 + \cdots + \lambda_{n-1} a_{n-1} = 0. \tag{11}$$

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

$$(t-a)^n = a_{-1} + a_0 t + \cdots + a_{n-1} t^n$$

we see that the quantity $\lambda_{-1} a_{-1} + \cdots + \lambda_{n-1} a_{n-1}$ 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 (11) 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. □

Proof of Theorem 8.1. Applying Proposition 8.2, 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 $\{0, 1, \ldots, n\}$, and since we may find at most $2n$ different degrees in S^2, Proposition 6.2 implies that

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

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

$$1, p_2, p_3, \ldots, p_n$$

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

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

where $S_i = S_{i-1} + K p_i$ for $i \geqslant 2$. We shall prove by induction on k that for $k = 3, 4, \ldots, n$, the space S_k has, possibly after changing the variable t, a basis of the form $1, (t+\alpha)t, \ldots, (t+\alpha)t^{k-1}$, 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 needed 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 α, 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, $3 \leqslant k \leqslant n-1$, 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 $0, 2, 3, \ldots, 2n$, which implies that T_k cannot be equal to the whole space of polynomials of degree at most $k+1$ so that $\dim T_k \leqslant k+1$. Notice also that T_k contains

$$1, (t+\alpha)t, (t+\alpha)t^2, \ldots, (t+\alpha)t^{k-1} \tag{12}$$

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 $\dim T_k \leqslant k+1$, a basis of T_k is therefore given by (12) 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. □

Theorem 8.1 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 8.3. *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 $G = r_1P_1 + \cdots + r_sP_s$. Denote by $\oplus$ the group law on the elliptic curve. Let $P = r_1P_1 \oplus \cdots \oplus r_sP_s$. From [15, 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 [15, Theorem 4.10 (a)]), hence there exists $R \in E$ such that $P = dR$. Therefore:

$$G - dO \sim d(R - O) \quad \Longrightarrow \quad G \sim dR. \qquad \square$$

Remark 8.4. According to the proof, the point R may not be 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 $\{0, -2, -3, \ldots, -n\}$, which can be easily derived from the Riemann–Roch Theorem. Multiplication by f only translates the sequence of valuations.

9. Function fields over non-algebraically closed fields

In this section we generalise Theorems 4.2, 5.3 and 6.3 to non-algebraically closed, perfect fields K. Recall that a field K is called *perfect* if all algebraic extensions of K are separable.

Theorem 9.1. *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*

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

Proof. 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'. ([16, Proposition III.6.1][(1)]). 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

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

by applying Theorem 4.2. □

We remark that the above proof has only used that any finite extension of K is generated by a single element, so that Theorem 9.1 actually holds in this somewhat more general case.

Theorem 9.2. *Let K be a perfect field, algebraically closed in an extension field F. Let $S \subseteq F$, $1 \in S$, be a space of finite dimension n and combinatorial genus γ.*

1. *If $n \geqslant 3$ and $\gamma = 0$, then S has genus 0 and $S = L(D)$ for D a divisor of degree $n-1$.*
2. *If $n \geqslant 4$ and $\gamma = 1$ then S has genus 0 or 1. Moreover,*
   (a) *if S has genus 1 then $S = L(D)$ for D a divisor of degree n,*
   (b) *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.*

Before proving Theorem 9.2, let us remind the reader of some basic facts concerning algebraic extensions of function fields that we need to call upon. We refer the reader to [16, Chapter III] for more background. Let F'/K' be an algebraic extension of F/K, meaning that $F' \supset F$ is an algebraic extension and that $K' \supset K$. Recall that if P is a place of F and P' a place of F' such that $P = F \cap P'$, P is said to *lie under* P' and P' to *lie over* P. One writes $P'|P$ to mean that P' lies over P. For any place P of F, there always exists at least a place P' over P ([16, Proposition III.1.7]), and for any such P and P' there exists ([16, Proposition III.1.4]) an integer $e = e(P'|P) \geqslant 1$ such that $v_{P'}(x) = e \cdot v_P(x)$ for any $x \in F$. The positive integer $e(P'|P)$ is called the *ramification index* of P' over P. The *conorm*, with respect to F'/F, of a place P of F is defined as the divisor:

$$Con_{F'/F}(P) = \sum_{P'|P} e(P'|P)P'.$$

The conorm extends to divisors $D = \sum_P \alpha_P P$ of F through the formula

$$Con_{F'/F}(D) = \sum_P \alpha_P Con_{F'/F}(P).$$

(1) The context of the proposition is that of functions fields of one variable, but its proof applies verbatim to arbitrary field extensions.

Proof of Theorem 9.2. Without loss of generality assume $F = K(S)$. Let K' be the algebraic closure of K and let $F' = K'(S)$ be defined inside the algebraic closure of F. We note that such an extension F'/F is unramified ([16, Theorem III.6.3 (a)]), meaning that $e(P'|P) = 1$ for any place P in F and any P' above it.

As remarked at the end of the proof of Theorem 9.1, K-linearly independent elements of F are also K'-linearly independent in F', therefore $\dim_K S = \dim_{K'} K'S$ and $\dim_K S^2 = \dim_{K'}(K'S)^2$, so that $K'S$ has combinatorial genus γ. Next, Theorems 5.3 (case $\gamma = 0$) and 6.3 (case $\gamma = 1$) apply to $K'S$ in the extension F'/K'.

Recall (Definition 7.2) that

$$D_S = \sum_{P, \text{ place of } F} - \min v_P(S) P$$

is such that $L(D_S)$ is the Riemann–Roch space in F of smallest dimension that contains S. By [16, Theorem III.6.3 (b)], F/K and F'/K' have the same genus g. It remains therefore only to prove that

$$\dim_K L(D_S) = \dim_{K'} L(D_{K'S}). \tag{13}$$

Let P be any place in the support of D_S, For any place P' above P we have $v_{P'}(s) = e(P'|P)v_P(s) = v_P(s)$ (since F'/F is unramified), therefore P' appears in the support of $D_{K'S}$. Furthermore, $v_{P'}(s) = v_P(s)$ for every $s \in S$, so that

$$\min_{s \in S} v_P(s) = \min_{s \in S} v_{P'}(s) = \min_{x \in K'S} v_{P'}(x)$$

since any K'-linear combination of elements of S has a P'-valuation at least equal to $\min_{s \in S} v_{P'}(s)$. Therefore, the coefficient in $D_{K'S}$ of every place P' above P equals exactly the coefficient of P in D_S.

Since any place P' of F' has a unique place P lying under it in F, we deduce that we have

$$Con_{F'/F}(D_S) = D_{K'S}$$

from which (13) follows by [16, Theorem III.6.3 (d)]. □

We conclude by remarking that when K is not algebraically closed, statement (1) of Theorem 9.2 is the correct generalisation of Theorem 5.3. Indeed, there exist spaces S of combinatorial genus 0 in extensions F/K, where K is algebraically closed in F, and such that S does not have a basis in geometric progression. One such example, given in [1], is obtained by considering the field $F = \mathbf{Q}(x, y)$, where $\mathbf{Q}$ denotes the rational field, and y is algebraic over $\mathbf{Q}(x)$ such that $y^2 + x^2 + 1 = 0$. We have that $\mathbf{Q}$ is algebraically closed in F, and in the extension $F/\mathbf{Q}$, the space S generated by $1, x, y$ has combinatorial genus 0 but can be seen not to have a basis in geometric progression. The space S is however equal to a Riemann–Roch space $L(P)$, where P is a place of degree 2. When one extends the base field $\mathbf{Q}$ to the complex field $\mathbf{C}$, we have that $\mathbf{C}S$ has the basis $t^{-1}, 1, t$, where $t = x + iy$,$t^{-1} = -x + iy$. Hence $\mathbf{C}S = L(P_0 + P_\infty)$, where P_0 and P_∞ are the places at 0 and at ∞ in $\mathbf{C}F = \mathbf{C}(t)$, and are the two places that lie above P in $\mathbf{C}F$.

Finally, we remark that the argument spelt out in the proof of Theorem 9.2 shows that if Conjecture 2.2 holds, then it also holds for perfect base fields.

References

[1] C. Bachoc, C. Serra, and G. Zémor, *An analogue of Vosper's theorem for extension fields*, Math. Proc. Philos. Soc. **163** (2017), 423–452.

[2] Christine Bachoc, Oriol Serra, and Gilles Zémor, *Revisiting Kneser's theorem for field extensions*, Combinatorica (2017), `https://doi.org/10.1007/s00493-016-3529-0`.

[3] V. Beck and C. Lecouvey, *Additive combinatorics methods in associative algebras*, To appear in Confluentes Math. ArXiv:math/1504.02287, 2015.
[4] N. Bourbaki, *éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations*, Actualités Scientifiques et Industrielles, No, Hermann, Paris, 1964.
[5] S. Eliahou and C. Lecouvey, *On linear versions of some addition theorems*, Linear Multilinear Algebra **57** (2009), 759–775.
[6] G. A. Freiman, *Foundations of a structural theory of set addition*, Transl. Math. Monogr., vol. 37, Amer. Math. Soc., Providence, R. I., 1973.
[7] William 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] Y. O. Hamidoune and Ø. Rødseth., *An inverse theorem modulo p*, Acta Arith. **92** (2000), 251–262.
[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] M. Kneser, *Summenmengen in Lokalkompakten Abelesche Gruppen*, Math. Z. **66** (1956), 88–110.
[11] Diego Mirandola and Gilles Zémor, *Critical pairs for the product singleton bound*, IEEE Trans. Inform. Theory **61** (2015), no. 9, 4928–4937.
[12] David Mumford, *Varieties defined by quadratic equations*, in Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970, pp. 29–100.
[13] Hugues Randriambololona, *On products and powers of linear codes under componentwise multiplication*, in Algorithmic arithmetic, geometry, and coding theory, Contemp. Math., vol. 637, Amer. Math. Soc., Providence, RI, 2015, pp. 3–78.
[14] R. M. Roth, N. Raviv, and I. Tamo, *Construction of Sidon spaces with applications to coding*, IEEE Trans. Inform. Theory **64** (2018), no. 6, 4412–4422.
[15] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[16] Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Grad. Texts in Math., vol. 254, Springer-Verlag, Berlin, 2009.
[17] Terence Tao and Van Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., vol. 105, Cambridge University Press, Cambridge, 2006.
[18] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc **31** (1956), 200–205.

Christine Bachoc, Institut de Mathématiques de Bordeaux, CNRS UMR 5251, Université de Bordeaux, 351 cours de la Libération, 33400 Talence, France
E-mail : christine.bachoc@math.u-bordeaux.fr

Alain Couvreur, INRIA & Laboratoire LIX, CNRS UMR 7161, École Polytechnique, Université Paris Saclay, 91128 Palaiseau Cedex, France
E-mail : alain.couvreur@lix.polytechnique.fr

Gilles Zémor, Institut de Mathématiques de Bordeaux, CNRS UMR 5251, Université de Bordeaux, 351 cours de la Libération, 33400 Talence, France
E-mail : gilles.zemor@math.u-bordeaux.fr