GENERATING SUBSPACE LATTICES, THEIR DIRECT PRODUCTS, AND THEIR DIRECT POWERS

GÁBOR CZÉDLI

Dedicated to Honorary Professor József Németh on his eightieth birthday

ABSTRACT. In 2008, László Zádori proved that the lattice $\mathrm{Sub}(V)$ of all subspaces of a vector space V of finite dimension at least 3 over a finite field F has a 5-element generating set; in other words, $\mathrm{Sub}(V)$ is 5-generated. We prove that the same holds over every 1- or 2-generated field; in particular, over every field that is a finite degree extension of its prime field. Furthermore, let F, t, V, $d \geq 3$, $\lfloor d/2 \rfloor$, and m denote an arbitrary field, the minimum cardinality of a generating set of F, a finite dimensional vector space over F, the dimension (assumed to be at least 3) of V, the integer part of $d/2$, and the least cardinal such that $m\lfloor d^2/4 \rfloor$ is at least t, respectively. We prove that $\mathrm{Sub}(V)$ is $(4+m)$-generated but none of its generating sets is of size less than m. Moreover, the k-th direct power of $\mathrm{Sub}(V)$ is $(5+m)$-generated for many positive integers k; for all positive integers k if F is infinite. Finally, let n be a positive integer. For $i = 1, \ldots, n$, let p_i be a prime number or 0, and let V_i be the 3-dimensional vector space over the prime field of characteristic p_i. We prove that the direct product of the lattices $\mathrm{Sub}(V_1)$, ..., $\mathrm{Sub}(V_n)$ is 4-generated if and only if each of the numbers p_1, ..., p_n occurs at most four times in the sequence p_1, ..., p_n. Neither this direct product nor any of the subspace lattices $\mathrm{Sub}(V)$ above is 3-generated.

1. NOTE ON THE DEDICATION

At the beginning of my university studies, Dr. József Németh taught me in the first semester. He was excellent. All the students in the classroom regretted that he was assigned different sections and courses for the next semester. As I reminisce about his unsurpassable tutorials, I wish him a happy birthday.

2. INTRODUCTION

For a lattice or a field A, we define the following cardinal number:

$$f^{\mathrm{mng}}(A) := \min\{|X| : X \text{ is a generating set of } A\}. \tag{2.1}$$

For later reference, note that for a field F,

$$F \text{ is a prime field if and only if } f^{\mathrm{mng}}(F) = 0. \tag{2.2}$$

1991 *Mathematics Subject Classification.* 06B99, 06C05.

Key words and phrases. Small generating set, four element generating set, subspace lattice, projective space, coordinatization of lattices, field extension.

This research was supported by the National Research, Development and Innovation Fund of Hungary, under funding scheme K-138892. **January 17, 2024.**

By a *field* we mean a *commutative field*. Let L be the subspace lattice of a vector space V of finite dimension $d \geq 3$ over a field F; in notation,

$$L := \mathrm{Sub}({}_F V), \text{ where } V = {}_F F^d \text{ is } 3 \leq d\text{-dimensional.} \tag{2.3}$$

We often write $\mathrm{Sub}(V)$ instead of $\mathrm{Sub}({}_F V)$. Zádori [22] proved that whenever F is a finite field, then L in (2.3) is 5-generated. Earlier, Gelfand and Ponomarev [7] proved that L is 4-generated but not 3-generated if F is a prime field; see Zádori [22] for historical details.

Our aim is to generalize these two results and prove some related results. In Zádori's result, F is a finite field with $f^{\mathrm{mng}}(F) = 1$; we remove finiteness from his assumptions on F and, instead of $f^{\mathrm{mng}}(F) = 1$, we assume only that $f^{\mathrm{mng}}(F) \in \{1, 2\}$. Related to Gelfand and Ponomarev' result, we prove that if $d = 3$ and F is a prime field, then $f^{\mathrm{mng}}(L^k) = 4$ holds for L from (2.3) even for $k \in \{2, 3, 4\}$ (in addition to $k = 1$); the number 4 is optimal here at both of its occurrences. Furthermore, we extend this result to direct products; so the just-mentioned result (for k-th direct powers, $k \in \{1, 2, 3, 4\}$) becomes a particular case. If no peculiarity of the (finite or infinite) cardinal number $f^{\mathrm{mng}}(F)$ is assumed and L is still from (2.3), then denote by m the smallest cardinal number such that $m\lfloor d^2/4 \rfloor \geq f^{\mathrm{mng}}(F)$. We prove that $m \leq f^{\mathrm{mng}}(L) \leq 4 + m$ and $f^{\mathrm{mng}}(L^k) \leq 5 + m$ for many integers $k \in \mathbb{N}^+ := \{1, 2, 3, \dots\}$; for all $k \in \mathbb{N}^+$ if F is infinite.

By a *nontrivial lattice* we mean an at least 2-element lattice. In Section 5, to shed more light on $f^{\mathrm{mng}}(L^k)$, we prove the following observation, in which L need not be a subspace lattice.

Observation 2.1. *Let L be a nontrivial lattice and let $n \in \mathbb{N}^+ := \{1, 2, 3, \dots\}$. If $k \in \mathbb{N}^+$ is large enough to exclude the existence of a k-element antichain in L^n, then L^k is not n-generated. In particular, L^k is not n-generated if $k > |L|^n$.*

Finally, note that in addition to earlier results on the generation of subspace lattices, a possible connection with cryptology also motivates the study of small generating sets of lattices; see Czédli [3].

Outline. Section 3 formulates exactly the results mentioned so far in three theorems, and presents some related statements. Section 4 recalls some well-known basic facts from coordinatization theory. Each of Sections 5, 6, and 7 proves one of the three theorems together with some auxiliary statements. Section 8 points out how one can extract Gelfand and Ponomarev's result, quoted right after (2.3), from Zádori's proof given in [22]. Section 9 presents two Maple programs related to Sections 3 and 6.

3. The main results and some of their corollaries

Recall that for $0 \leq r \leq m \in \mathbb{N}^+$ and a prime power q, the *Gaussian binomial coefficient* is defined as

$$\binom{m}{r}_q := \frac{(1-q^m)(1-q^{m-1})\cdots(1-q^{m-r+1})}{(1-q)(1-q^2)\cdots(1-q^r)}; \tag{3.1}$$

see, e.g., O'Hara [16][1]. For convenience, let us agree that for a cardinal λ,

$$\text{if } 1 \leq r \leq m-1 \in \mathbb{N}^+ \text{ and } \lambda \geq \aleph_0, \text{ then we let } \binom{m}{r}_\lambda := \lambda. \tag{3.2}$$

[1] https://en.wikipedia.org/wiki/Gaussian_binomial_coefficient would also do.

This convention is motivated by the fact that (3.1) is known to be the number of the r-dimensional subspaces of the[2] m-dimensional vector space over the q-element field; now the same holds for every λ-element field in virtue of (3.2). The upper integer part and the lower integer part of a real number x will be denoted by $\lceil x \rceil$ and $\lfloor x \rfloor$, respectively; for example, $\lceil \sqrt{80} \rceil = \lceil 9 \rceil = 9$ and $\lfloor \sqrt{80} \rfloor = \lfloor 8 \rfloor = 8$. More generally, let us agree that for a cardinal number t and a positive integer n,

$$\lceil t/n \rceil := \min\{m : mn \geq t\};\ \text{it is a cardinal number.} \tag{3.3}$$

Theorem 3.1. *As in* (2.3)*, assume that* $L = \mathrm{Sub}({}_FV)$*, where* F *is an arbitrary field,* $3 \leq d \in \mathbb{N}^+$*, and* V *is the* d*-dimensional vector space over* F*. Let* $t := f^{\mathrm{mng}}(F)$*, the minimum of the cardinalities of the generating sets of* F*; see* (2.1)*. Then*

$$4 \leq f^{\mathrm{mng}}(L) \leq 4 + \Big\lceil \frac{t}{\lfloor d^2/4 \rfloor} \Big\rceil. \tag{3.4}$$

For $t = 0$ or $t \in \{1, 2\}$, (3.4) implies that $f^{\mathrm{mng}}(L) = 4$ or $f^{\mathrm{mng}}(L) \leq 5$, respectively. Thus, the results quoted from Zádori [22] and Gelfand and Ponomarev [7] after (2.3) are particular cases of Theorem 3.1. Note that

$$\lfloor d^2/4 \rfloor = \lfloor d/2 \rfloor \cdot \lceil d/2 \rceil \text{ and so } \Big\lceil \frac{t}{\lfloor d^2/4 \rfloor} \Big\rceil = \Big\lceil \frac{t}{\lfloor d/2 \rfloor \cdot \lceil d/2 \rceil} \Big\rceil \tag{3.5}$$

hold for $3 \leq d \in \mathbb{N}^+$. If t is large compared to d, then (3.6) below gives a better lower bound for $f^{\mathrm{mng}}(L)$ than the first inequality in (3.4).

Theorem 3.2. *Let* F *be a field, let* $3 \leq d \in \mathbb{N}^+$*, and denote by* V *and* L *the* d*-dimensional vector space over* F *and its subspace lattice* $\mathrm{Sub}({}_FV)$*, respectively. Let* $k \in \mathbb{N}^+$ *and, with reference to* (3.1) *and* (3.2)*, let*

$$\mu := \binom{d}{\lfloor d/2 \rfloor}_{|F|}. \tag{3.6}$$

Then, using the notations of (2.1)*,* (2.2)*,* (3.3)*, and* (3.4) *and letting* $t := f^{\mathrm{mng}}(F)$*, the following inequalities and equalities hold for* $f^{\mathrm{mng}}(L)$ *and* $f^{\mathrm{mng}}(L^k)$*:*

$$\Big\lceil \frac{t}{\lfloor d^2/4 \rfloor} \Big\rceil \leq f^{\mathrm{mng}}(L) \leq f^{\mathrm{mng}}(L^k), \tag{3.7}$$

$$\text{if } k \leq \mu, \quad \text{then} \quad f^{\mathrm{mng}}(L^k) \leq 5 + \Big\lceil \frac{t}{\lfloor d^2/4 \rfloor} \Big\rceil, \tag{3.8}$$

$$f^{\mathrm{mng}}(L^k) = 4 \text{ provided that } t = 0,\ d = 3, \text{ and } k \in \{1, 2, 3, 4\}, \text{ and} \tag{3.9}$$

$$f^{\mathrm{mng}}(L^k) = 5 \text{ provided that } t = 0,\ d = 3,\ k \in \mathbb{N}^+, \text{ and } 5 \leq k \leq \mu. \tag{3.10}$$

As μ can be an infinite cardinal number, (3.10) repeats that $k \in \mathbb{N}^+$.

Theorem 3.3. *Let* λ *be a nonzero ordinal number, and assume that for each* $\iota < \lambda$*,* V_ι *is the* 3*-dimensional vector space over a prime field* F_ι*. Let* L *be the direct product of the corresponding subspace lattices, that is,*

$$L := \prod_{\iota < \lambda} \mathrm{Sub}(V_\iota). \tag{3.11}$$

Then $f^{\mathrm{mng}}(L) = 4$ *if and only if* λ *is finite,* $\lambda \neq 0$*, and, up to isomorphism, each prime field occurs at most four times in the sequence* $(F_\iota : \iota < \lambda)$*.*

[2]As the definite article indicates, the m-dimensional vector space over a given field in the paper is understood up to isomorphism but its subspaces are not.

It does not seem to be easy to generalize (3.9) and (3.10) to $3 < d \in \mathbb{N}^+$. Table 1, obtained by computer algebra[3], shows that the Gaussian binomial coefficient μ occurring in (3.6) is large in general.

$q =$	2	3	4	5
$\mu \approx$	$1.540 \cdot 10^{482}$	$4.423 \cdot 10^{763}$	$2.871 \cdot 10^{963}$	$2.958 \cdot 10^{1118}$
$q =$	7	8	9	11
$\mu \approx$	$1.715 \cdot 10^{1352}$	$1.023 \cdot 10^{1445}$	$7.002 \cdot 10^{1526}$	$1.878 \cdot 10^{1666}$
$q =$	13	16	17	19
$\mu \approx$	$2.223 \cdot 10^{1782}$	$4.186 \cdot 10^{1926}$	$5.574 \cdot 10^{1968}$	$1.073 \cdot 10^{2046}$

TABLE 1. For $d = 80$, the approximate values of some Gaussian binomial coefficients occurring in (3.6)

The following remark is trivial since L^h and $\prod_{i\in S} L_i$ in it are homomorphic images of L^k and $\prod_{i\in[k]} L_i$ (where $[k] = \{1, \dots, k\}$), respectively.

Remark 3.4. For a lattice L and $h, k, n \in \mathbb{N}^+$ such that $h < k$, if L^k is n-generated, then $f^{\mathrm{mng}}(L^h) \leq n$. More generally, if $\prod_{i\in[k]} L_i$ is n-generated and $S \subseteq [k]$, then $\prod_{i\in S} L_i$ has an at most n-element generating set.

The following easy lemma could be of separate interest. For a subset X of a vector space V over a field K, let $\mathrm{Span}_K(X)$ denote the subspace of V generated by X; we can also write $\mathrm{Span}(X)$ if K is clear from the context.

Lemma 3.5. *Let F be a field with a subfield P (that is, let $F|P$ be a field extension) and let $3 \leq d \in \mathbb{N}^+$. Furthermore, let $V' = {}_P P^d$ and $V = {}_F F^d$ be the d-dimensional vector spaces (consisting of d-tuples) over P and F, respectively. Then*

$$\varphi\colon \mathrm{Sub}({}_P V') \to \mathrm{Sub}({}_F V), \text{ defined by } X \mapsto \mathrm{Span}_F(X), \tag{3.12}$$

is a lattice embedding. Furthermore, φ preserves the length, the covering relation, the smallest element 0, and the largest element 1. We also have that for any subset H of V', $\varphi(\mathrm{Span}_P(H)) = \mathrm{Span}_F(H)$.

In the forthcoming Example 3.6, to be proved in Section 7, the number 80 makes one and a half dozen appearances. Although most instances could be replaced by any positive integer greater than 1, we have opted for 80 in keeping with the paper's dedication.

Example 3.6. Let F be a field and let $3 \leq d \in \mathbb{N}^+$. Let L stand for the subspace lattice $\mathrm{Sub}(V) = \mathrm{Sub}({}_F F^d)$ of the d-dimensional vector space V over F. Then the following six assertions hold.

(a) If $\alpha_1, \dots, \alpha_{80}$ are (not necessarily distinct) algebraic irrational numbers over the field $\mathbb{Q}$ of rational numbers and $F = \mathbb{Q}(\alpha_1, \dots, \alpha_{80})$ is the field that these numbers generate, then L has a 5-element generating set. Furthermore, for every $2 \leq k \in \mathbb{N}^+$, L^k has a 6-element generating set. In particular, if

$$F = \mathbb{Q}\bigl(\sqrt{2023}, \sqrt{2}, \sqrt[3]{3}, \sqrt[4]{4}, \sqrt[5]{5}, \sqrt[6]{6}, \dots, \sqrt[80]{80}\,\bigr),$$

then L^{80} has a 6-element generating set.

[3]Maple V, see Footnote 11 for more details, but many others would also do.

(b) Let $\beta_1, \ldots, \beta_{80}$ be algebraically independent transcendental numbers over $\mathbb{Q}$ and let $F := \mathbb{Q}(\beta_1, \ldots, \beta_{80})$. If $d = 3$, then L has a 44-element generating set and each of its generating sets consists of at least 40 elements. If $d = 8$, then L has a 9 element generating set but not a 4-element one.

(c) If $\gamma_1, \ldots, \gamma_{80}$ are algebraically independent transcendental numbers over $\mathbb{Q}$, $F = \mathbb{Q}(\gamma_1, \ldots, \gamma_{80})$, $d = 80^{80}$, and $k = 80^{80d}$, then L has a 5-element generating set and L^k has a 6-element one.

(d) If $|F| = 19$ or $F = \mathbb{Q}$, $d = 80$, and $k = 10^{2046}$, then L^k can be generated by five elements.

(e) If $F = \mathbb{A}$, the field of algebraic numbers, then L is not finitely generated.

(f) If $F = \mathbb{Q}(\pi^{80}, \sqrt[80]{80})$, where $\pi \approx 3.141\,592\,653\,589\,793$ is the well-known transcendental constant, then L has a 5-element generating set while L^{80} has a 6-element one.

Remark 3.7. For $F = \mathbb{Q}(\pi^{80}, \sqrt[80]{80})$ in Example 3.6(f), $f^{\mathrm{mng}}(F) = 2$.

4. Some basic facts from the coordinatization theory of lattices

The proof of Theorem 3.1 grew out from the coordinatization theory of Arguesian lattices. This theory was introduced by J. von Neumann; see, for example, Artmann [1], Day and Pickering [5], Freese [6], Herrmann [9] and [10], and von Neumann [14, 15]. As these papers but Herrmann [9] and [14] are referenced in Czédli and Skublics [4], where the treatment and the notations are unified, it will be convenient to reference also [4][4] even though no result that was first proved in [4] is needed here. Actually, we need only the easy first step from coordinatization theory, and the statements of this section are straightforward to verify with elementary computations in Linear Algebra. In the paper, we often use the notation

$$[i] := \{1, 2, \ldots, i\} \text{ for } i \in \mathbb{N}_0; \text{ in particular, } [0] := \emptyset.$$

As a general assumption for the whole section, we assume that F is a field, $3 \leq d \in \mathbb{N}^+$, and $V = {}_F F^d$ is the d-dimensional vector space over F. We let $v_i := (0, \ldots, 0, 1, 0, \ldots, 0) \in V$, with 1 at the i-th position, for $i \in [d]$. We turn $V = {}_F F^d$ into the $(d-1)$-dimensional projective space $P_{d-1} = P_{d-1}(F)$ over F in the usual way except that we use -1 instead of 1 for "finite" points[5]; see, e.g., Figure 1.

The points and the lines of P_{d-1} are the 1-dimensional subspaces and the 2-dimensional subspaces of V, respectively. A 1-dimensional subspace of V is either of the form $F(x_1, \ldots, x_{d-1}, -1)$ and then $[x_1, \ldots, x_{d-1}, -1]$ denotes (in other words, coordinatizes) the corresponding (*projective*) *point* of P_{d-1}, or this subspace is of the form $F(x_1, \ldots, x_{d-1}, 0)$ and then $[x_1, \ldots, x_{d-1}, 0]$ stands for the corresponding projective point. We call the points of the form $[x_1, \ldots, x_{d-1}, 0]$ *points at infinity* (even if F is finite and thus so is P_{d-1}); the rest of the points are said to by *finite points*. The finite points form the $(d-1)$-dimensional affine space over F. As usual, this affine space visualizes P_{d-1} so that the finite points are the points of the affine space, while an infinite projective point $[x_1, \ldots, x_{d-1}, 0]$ is the *direction*

[4]At the time of writing, a preprint of this paper is freely available from http://tinyurl.com/czedli-skublics or, equivalently, it can be found in the author's website, https://www.math.u-szeged.hu/ czedli/ = http://tinyurl.com/g-czedli .

[5]The -1 is explained by the minus sign in von Neumann's choice of $c_{i,j} = F(v_i - v_j)$, see later, and by our intention that the unit $c_{1,4}$ of $R\langle 4, 1\rangle$, to be defined soon, in Figure 2 should be to the right of the zero a_4 of the ring.

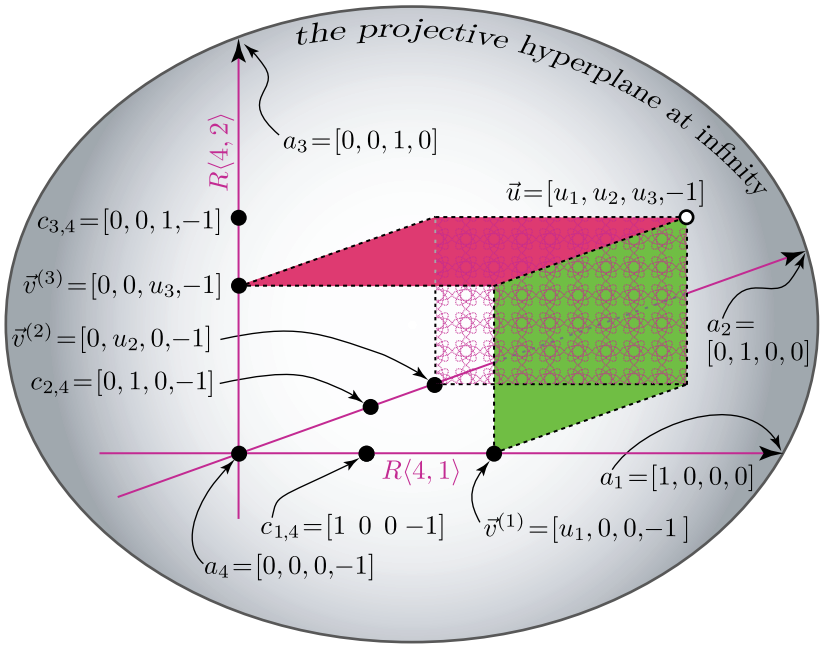

FIGURE 1. The 3-dimensional projective space

$(x_1,\dots,x_{d-1})$ in the affine space. (Of course, $(\lambda x_1,\dots,\lambda x_{d-1})$ is the same direction and $[\lambda x_1,\dots,\lambda x_{d-1},0]$ is the same projective point at infinity for any $\lambda\in F\setminus\{0\}$.) Some sort of visualization of P_{d-1} for $d=4$ is given in Figure 1; most parts of this figure will be used only later.

We often consider the projective space P_{d-1} and a line h of P_{d-1} as the set of all points of P_{d-1} and the set of points lying on h. For points $x\neq y$ in P_{d-1}, let $\ell_{x,y}$ denote the unique line through x and y. Following, say, Grätzer [8, page 376], a subset X of P_{d-1} is said to be a *subspace* of P_{d-1} if whenever x and y are distinct points in X, then X contains all points of the line $\ell_{x,y}$. The subspaces of P_{d-1} form a lattice, which we denote by $\mathrm{Sub}(P_{d-1})=\bigl(\mathrm{Sub}(P_{d-1});\subseteq\bigr)$. For convenience (and following the traditions), if x and y are distinct points of P_{d-1}, then we often write $x\vee y$ instead of $\ell_{x,y}$, and we usually write $x\in\mathrm{Sub}(P_{d-1})$ instead of the more precise $\{x\}\in\mathrm{Sub}(P_{d-1})$. When we think of their coordinates, we denote the points of P_{d-1} by $\vec{x}$, $\vec{u}$, etc.. There is a well-known isomorphism η from $L=\mathrm{Sub}({}_FV)$ to the subspace lattice $\mathrm{Sub}(P_{d-1})$. Namely, $\eta\colon L\to\mathrm{Sub}(P_{d-1})$ is defined by the rule

$$\eta(X):=\{P\in P_{d-1}:\text{the point }P\text{ corresponds to a}\\ \text{1-dimensional subspace of }X\}\in\mathrm{Sub}(P_{d-1}) \tag{4.1}$$

for $X\in\mathrm{Sub}({}_FV)$. We do not make a sharp distinction between X and $\eta(X)$. We use $\eta(X)$ and the projective space to explain and visualize the proofs. The respective (and straightforward) computations can be done with X in $\mathrm{Sub}({}_FV)$ or with $\eta(X)$ in $P_{d-1}=P_{d-1}(F)$ based on the following fact, which is well known and it can easily be derived from (4.1). As in Neumann [15] and in Example 2.1 right after (2.3) in [4], the components of the (*canonical* (*extended normalized von*

Neumann)) *d-frame*

$$\vec{f} = (\vec{a}, \vec{c}) = \big((a_1, \dots, a_d),\, (c_{i,j} : i, j \in [d],\, i \neq j)\big) \tag{4.2}$$

are the 1-dimensional subspaces $a_i = Fv_i \in V \in \mathrm{Sub}({}_FV)$ for $i \in [d]$ and $c_{i,j} = F(v_i - v_j)$ for $i \neq j \in [d]$ in $\mathrm{Sub}({}_FV)$. Thus, by (4.1), the components of $\vec{f}$ are the following points

$$a_i = [0, \dots, 0, 1, 0 \dots, 0] \text{ for } i \in [d-1],\ a_d = [0, \dots, 0, -1], \tag{4.3}$$

$$\text{and } c_{i,j} = [0, \dots, 0, 1, 0 \dots, 0, -1, 0, \dots, 0] \text{ for } i \neq j \in [d], \tag{4.4}$$

where the unit 1 is at the i-th position in both cases and the -1 is at the j-th position, in $\mathrm{Sub}(P_{d-1})$. Note that $c_{i,j} = c_{j,i}$ for $i, j \in [d]$ distinct but, according to (4.4), their *canonical forms* are different[6].

For $i, j, k \in [d]$ pairwise distinct, repeating what von Neumann and his followers did but using the notation of [4, (2.5)], the (i, j)-th *coordinate ring* of L with respect to $\vec{f}$ is

$$R\langle i, j\rangle = R\langle a_i, a_j\rangle := \{x \in L : x \vee a_j = a_i \vee a_j,\ x \wedge a_j = 0\}. \tag{4.5}$$

To define the ring operations, we need the following *projectivities* from Neumann [15]; we use the visual notation from Czédli and Skublics [4]. So for pairwise distinct parameters $p, q, r \in [d]$, let

$$F\left(\begin{smallmatrix} p & q \\ r & q \end{smallmatrix}\right) \colon [0, a_p \vee a_q] \to [0, a_r \vee a_q], \quad x \mapsto (x \vee c_{p,r}) \wedge (a_r \vee a_q), \tag{4.6}$$

$$F\left(\begin{smallmatrix} p & q \\ p & r \end{smallmatrix}\right) \colon [0, a_p \vee a_q] \to [0, a_p \vee a_r], \quad x \mapsto (x \vee c_{q,r}) \wedge (a_p \vee a_r). \tag{4.7}$$

For $i, j, k \in [d]$ pairwise distinct and $x, y \in R\langle i, j\rangle$, we let

$$x \oplus_{ijk} y := (a_i \vee a_j) \wedge \Big(\big((x \vee a_k) \wedge (c_{i,k} \vee a_j)\big) \vee F\left(\begin{smallmatrix} i & j \\ k & j \end{smallmatrix}\right)(y)\Big), \tag{4.8}$$

$$x \otimes_{ijk} y := (a_i \vee a_j) \wedge \Big(F\left(\begin{smallmatrix} i & j \\ i & k \end{smallmatrix}\right)(x) \vee F\left(\begin{smallmatrix} i & j \\ k & j \end{smallmatrix}\right)(y)\Big), \text{ and} \tag{4.9}$$

$$x \ominus_{ijk} y := (a_i \vee a_j) \wedge \Big(a_k \vee \big((c_{j,k} \vee x) \wedge (a_j \vee F\left(\begin{smallmatrix} i & j \\ i & k \end{smallmatrix}\right)(y))\big)\Big); \tag{4.10}$$

they are in $R\langle i, j\rangle$ and do not depend on k. Except that the lattice polynomials defined in (4.8), (4.9), and (4.10) as well as the projections defined in (4.6) and (4.7) are

$$\text{built from } \vee,\ \wedge, \text{ and the components of } \vec{f}, \tag{4.11}$$

their details are not relevant here, and there are other ways to define appropriate $\oplus$, $\otimes$, and $\ominus$. In fact, as Herrmann [10, 2 lines after Theorem 2.2] notes, Neumann used the opposite of $\otimes_{ijk}$. Fortunately, what we need from von Neumann's voluminous [15], has already been summarized in Herrmann [10, Theorem 2.2], in Section 2 of Czédli and Skublics, and (partially) in Freese [6, Page 284]. Furthermore, the isomorphism given in (4.1) allows us to pass from $\mathrm{Sub}({}_FF^d)$ to $\mathrm{Sub}(P_{d-1})$. So, based on (4.5)–(4.10), we can recall the following theorem.

Theorem 4.1 (von Neumann [15] for $3 \leq d \in \mathbb{N}^+$ and Day and Pickering [5] for $d = 3$)**.** *For $i, j \in [d]$ distinct, the operations defined in* (4.8), (4.9), *and* (4.10) *in $L = \mathrm{Sub}(P_{d-1})$ do not depend on $k \in [d] \setminus \{i, j\}$, and*

$$R(i, j) = \big(R(i, j); \oplus_{ijk}, \ominus_{ijk}, \otimes_{ijk}\big)$$

[6]When we consider $c_{i,j}$ an element of $R\langle j, i\rangle$, to be defined soon, then we use the canonical form given in (4.4).

is a ring, called the (i,j)-th coordinate ring, *for each $k \in [d] \setminus \{i,j\}$. The map $\delta_{d,1}\colon F \to R\langle d,1\rangle$ defined by $\delta_{d,1}(r) := [r,0,\dots,0,-1]$ is a ring isomorphism (and so it is a field isomorphism). So is the map $\delta_{i,j}\colon F \to R\langle i,j\rangle$ defined by*

$$\delta_{i,j}(r) := [0,\dots,0,r,0,\dots,0,-1,0,\dots,0] \in \mathrm{Sub}(P_{d-1}) \tag{4.12}$$

with r at the j-th position and -1 at the i-th position. Thus, the coordinate rings $R\langle i,j\rangle$, $i \neq j \in [d]$, are all isomorphic to the field F. The elements a_i and $c_{j,i}$ are the zero and the unit of $R\langle i,j\rangle$. The ring isomorphisms given in (4.12) *commute*[7] *with the projectivities defined in* (4.6) *and* (4.7)*, respectively. That is, for any $p,q,r \in [d]$ such that $|\{p,q,r\}| = 3$,*

$$F\left(\begin{smallmatrix} p & q \\ r & q \end{smallmatrix}\right) \circ \delta_{p,q} = \delta_{r,q} \quad \text{and} \quad F\left(\begin{smallmatrix} p & q \\ p & r \end{smallmatrix}\right) \circ \delta_{p,q} = \delta_{p,r}. \tag{4.13}$$

Furthermore, using the superscript ^{rest} to denote the restrictions of the projectivities occurring in (4.13) *to $R\langle p,q\rangle$,*

$$F\left(\begin{smallmatrix} p & q \\ r & q \end{smallmatrix}\right)^{rest}\colon R\langle p,q\rangle \to R\langle r,q\rangle \text{ is a ring isomorphism,} \tag{4.14}$$

$$\text{so is } F\left(\begin{smallmatrix} p & q \\ p & r \end{smallmatrix}\right)^{rest}\colon R\langle p,q\rangle \to R\langle p,r\rangle, \tag{4.15}$$

and (4.13) *remains true if we change the projections in it to their restrictions to $R\langle p,q\rangle$.*

5. Proving Theorem 3.1

A *generating vector* of a lattice L is a vector $\vec{b} = (b_1,\dots,b_s)$ of not necessarily distinct elements of L such that $\{b_1,\dots,b_s\}$ generates L.

Proof of Observation 2.1. We argue by way of contradiction. Suppose that k is large enough in the given sense but L^k has an n-dimensional generating vector $(\vec{b}^{(1)},\dots,\vec{b}^{(n)})$. For $i \in [k]$, let $\pi_i\colon L^k \to L$ denote the i-th projection defined by $\vec{x} \mapsto x_i$. Let $\vec{g}^{(i)} := (\pi_i(\vec{b}^{(1)}),\dots,\pi_i(\vec{b}^{(n)}) \in L^n$. As k is large, there are $i,j \in [k]$ such that $i \neq j$ and $\vec{g}^{(i)} \leq \vec{g}^{(j)}$, understood componentwise. Then for any n-ary lattice term f, we have that

$$\begin{aligned} \pi_i\bigl(f(\vec{b}^{(1)},\dots,\vec{b}^{(n)})\bigr) &= f\bigl(\pi_i(\vec{b}^{(1)}),\dots,\pi_i(\vec{b}^{(n)})\bigr) = f(\vec{g}^{(i)}) \\ \leq f(\vec{g}^{(j)}) &= f\bigl(\pi_j(\vec{b}^{(1)}),\dots,\pi_j(\vec{b}^{(n)})\bigr) = \pi_j\bigl(f(\vec{b}^{(1)},\dots,\vec{b}^{(n)})\bigr). \end{aligned} \tag{5.1}$$

As $(\vec{b}^{(1)},\dots,\vec{b}^{(n)})$ is a generating vector, (5.1) implies that $\pi_i(\vec{x}) \leq \pi_j(\vec{x})$ for every $\vec{x} \in L^k$, which is a contradiction completing the proof. □

Proof of Lemma 3.5. Since $V' \subseteq V$, (3.12) makes sense. For a subset $H \subseteq V'$, since the operation of spanning is order-preserving and idempotent,

$$\mathrm{Span}_F(H) \subseteq \mathrm{Span}_F(\mathrm{Span}_P(H)) \subseteq \mathrm{Span}_F(\mathrm{Span}_F(H)) = \mathrm{Span}_F(H)$$

and $\mathrm{Span}_F(\mathrm{Span}_P(H)) = \varphi(\mathrm{Span}_P(H))$ imply the last sentence of the lemma.

Let X be a subspace of V', denote its dimension by t, and take a maximal subset $U := \{\vec{a}^{(1)},\dots,\vec{a}^{(t)}\}$ of linearly independent vectors in X. Then, for $i \in [t]$, $\vec{a}^{(i)}$ is of the form $\vec{a}^{(i)} = (u_{i,1},\dots,u_{i,d})$ with entries from P, and the rank of the matrix $A := (u_{i,j})_{t\times d}$ is t. As U generates (in other words, linearly spans) X in V', the last sentence of the lemma gives that $Y := \mathrm{Span}_F(U)$ equals $\varphi(X)$. The rank t of A is captured by determinants, so it remains t when we pass from P to

[7] We compose maps from right to left; e.g., $(\alpha\beta)(x) = \alpha(\beta(x))$.

F. Hence, $\varphi(X) = Y$ is also of dimension t. Since both V' and V are of the same finite dimension d, it follows that φ is cover-preserving, $\varphi(0) = 0$, and $\varphi(1) = 1$. Denote the join in $\mathrm{Sub}({}_PV')$ and that in $\mathrm{Sub}({}_FV)$ by $\vee'$ and $\vee$, respectively. For $X, Y \in V'$, the last sentence of the lemma allows us to compute as follows:

$$\begin{aligned}\varphi(X \vee' Y) &= \varphi(\mathrm{Span}_P(X \cup Y)) = \mathrm{Span}_F(X \cup Y)\\ &= \mathrm{Span}_F(\mathrm{Span}_F(X) \cup \mathrm{Span}_F(Y))\\ &= \mathrm{Span}_F(\varphi(X) \cup \varphi(Y)) = \varphi(X) \vee \varphi(Y).\end{aligned}$$

Thus, φ is a join-homomorphism. We claim that if $X, Y \in \mathrm{Sub}({}_PV')$ such that $\varphi(X) \leq \varphi(Y)$, then $X \leq Y$. Suppose the contrary, that is, $\varphi(X) \leq \varphi(Y)$ but $X \not\leq Y$. Then $Y < X \vee' Y$ and $\varphi(Y) = \varphi(X) \vee \varphi(Y) = \varphi(X \vee' Y)$ together contradict the fact that φ is dimension-preserving. Therefore, $X \leq Y \iff \varphi(X) \leq Y$, that is, φ is an order-embedding. We know from Lemma 1 of Wild [20] that every cover-preserving order embedding between two lower semimodular lattices is a meet-embedding. Therefore, since subspace lattices are lower semimodular (in fact, they are even modular), we obtain that φ preserves the meets. Thus, φ is a lattice embedding, completing the proof of Lemma 3.5 □

The following observation is trivial by definitions.

Observation 5.1. *Let F be a field, $3 \leq d \in \mathbb{N}^+$, and let $\vec{u}^{(1)} = [u_1^{(1)}, \ldots, u_d^{(1)}]$, $\ldots$, $\vec{u}^{(k)} = [u_1^{(k)}, \ldots, u_d^{(k)}]$ be points in $P_{d-1}(F)$; according to our convention, we assume that $\{u_d^{(1)}, \ldots, u_d^{(k)}\} \subseteq \{0, -1\}$. Then a point $\vec{v} = [v_1, \ldots, v_d] \in P_{d-1}(F)$, with $v_d \in \{0, 1\}$ again, belongs to the subspace generated (in other words, spanned) by $\{\vec{u}^{(1)}, \ldots, \vec{u}^{(k)}\}$ if and only if there exist $\lambda_1, \ldots, \lambda_k \in F$ such that*

$$v_i = \sum_{j \in [k]} \lambda_j u_i^{(j)} \quad \text{for } i \in [d]. \tag{5.2}$$

If $\vec{v}$ is a finite point, that is, if $v_d = -1$, then (5.2) implies that $\Theta := \{i : u_d^{(i)} = -1\} \neq \emptyset$ and $\sum_{i \in \Theta} \lambda_i = 1$. If $\vec{v}$ and all the $\vec{u}^{(i)}$, $i \in [k]$, are finite points, then (5.2) means that $\vec{v}$ is a so-called affine combinations *of $\vec{u}^{(1)}$, $\ldots$, $\vec{u}^{(k)}$, that is, $\sum_{i \in [k]} \lambda_i = 1$.*

As $R\langle d, 1\rangle \cong F$ is a field, it is natural that we need the (partial) unary operation of forming reciprocals. By passing from Huhn diamonds, see Huhn [12], to our setting based on (von Neumann) frames, such a unary operation could be derived from any of the two division operations given at the bottom of Page 510 in Day and Pickering [5]. However, while [5] deals with a more general class of modular lattices, we need this unary operation only in the simple situation where our lattice is of the form $\mathrm{Sub}(P_{d-1})$ and $R\langle d, 1\rangle$ is determined by the canonical frame. Hence, and also because some details will be useful later, we define such a unary operation directly. Namely, for $i, j, k \in [d]$ pairwise distinct and $x \in \mathrm{Sub}(P_{d-1})$, we define

$$\begin{aligned}\mathrm{rec}_{ijk}(x) := \Big(\Big(\Big(\big((x \vee c_{k,i}) \wedge (a_j \vee a_k)\big) \vee c_{j,i}\Big)\Big)\\ \wedge (a_k \vee a_i) \vee c_{k,j}\Big) \wedge (a_i \vee a_j) \in R\langle i, j\rangle.\end{aligned} \tag{5.3}$$

Lemma 5.2. *If F is a field, $3 \leq d \in \mathbb{N}^+$, and $x \in R\langle i, j\rangle \subseteq \mathrm{Sub}(P_{d-1})$ such that $x \neq a_i$, then $\mathrm{rec}_{ijk}(x)$ is the reciprocal of x in $R\langle i, j\rangle$, that is, $x \otimes_{ijk} \mathrm{rec}_{ijk}(x) =$*

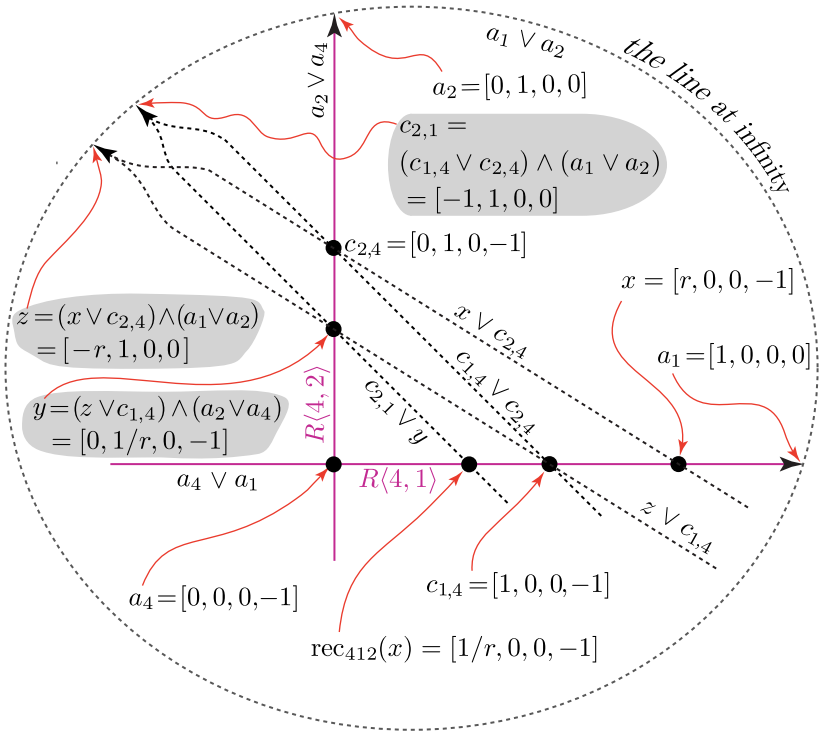

FIGURE 2. Computing reciprocals

$c_{j,i}$. *Furthermore,* $\mathrm{rec}_{ijk}(a_i) = a_j$ *and* (4.11) *is valid for* (5.3)*, too. (Note that* $a_j \notin R\langle i, j\rangle$ *and, by Theorem 4.1,* a_i *and* $c_{j,i}$ *are the zero* $0_{R\langle i,j\rangle}$ *and the unit* $1_{R\langle i,j\rangle}$ *in* $R\langle i, j\rangle$*, respectively.)*

Proof. We deal only with $(d, i, j, k) = (4, 4, 1, 2)$, which reflects the general case. The proof is given by Figure 2. To exemplify how this figure determines an easy formal argument in a straightforward way, we present only the following details; similar details from other proofs will be omitted. By Theorem 4.1, $x = \delta_{i,j}(r) = \delta_{4,1}(r) = [r, 0, 0, -1]$ for some $r \in F \setminus \{0\}$, and it suffices to show that $\mathrm{rec}_{412}(x) = \delta_{4,1}(1/r)$, that is, $\mathrm{rec}_{412}(x) = [1/r, 0, 0, -1]$. With $z := (x \vee c_{2,4}) \wedge (a_1 \vee a_2)$ and $y := (z \vee c_{1,4}) \wedge (a_2 \vee a_4)$, we have that $\mathrm{rec}_{412}(x) = (y \vee c_{2,1}) \wedge (a_4 \vee a_1)$. Assuming that $z = [-r, 1, 0, 0]$ is already known, we proceed to the next computation step. Namely, we verify that y is correctly given in the figure. Using $c_{1,4} = [1, 0, 0, -1]$, $c_{2,4} = [0, 1, 0, -1]$, $a_1 = [1, 0, 0, 0]$, $a_2 = [0, 1, 0, 0]$, and $a_4 = [0, 0, 0, -1]$ from (4.3)–(4.4), Observation 5.1 implies that a point P is in $z \vee c_{1,4}$ if and only if it is of the form $[-\beta_1 r + \beta_2, \beta_1, 0, -\beta_2]$ such that $\beta_1 \in F$, $\beta_2 \in \{0, 1\}$, and $(\beta_1, \beta_2) \neq (0, 0)$. Similarly, P is in $a_2 \vee a_4$ if and only if it is of the form $[0, \lambda_1, 0, -\lambda_2]$ such that $\lambda_1 \in F$, $\lambda_2 \in \{0, 1\}$, and $(\lambda_1, \lambda_2) \neq (0, 0)$. Comparing the two forms, we have that $\beta_1 = \lambda_1$, $\beta_2 = \lambda_2$, and $-\beta_1 r + \beta_2 = 0$. By the last equality and $r \neq 0$, we have that $\beta_1 \neq 0 \iff \beta_2 \neq 0$. So $(\beta_1, \beta_2 \neq (0, 0)$ and $\beta_2 \in \{0, 1\}$ give that $\beta_2 = 1$. Hence, $-\beta_1 r + \beta_2 = 0$ implies that $\beta_1 = 1/r$, and so $P = [0, 1/r, 0, -1]$. This computation verifies the equality $y = [0, 1/r, 0, -1]$, confirming the figure. □

Proof of Theorem 3.1. In virtue of the isomorphism given in (4.1), we can assume that $L = \mathrm{Sub}(P_{d-1}(F)) = \mathrm{Sub}(P_{d-1})$. Denoting the prime field of F by P, let $L' = \mathrm{Sub}(P_{d-1}(P))$. Let $\vec{f}'$ and $\vec{f}$ be the canonical frames in L' and L according to (4.3)–(4.4), respectively. The isomorphism given in (4.1) depends on the underlying field, this is why the next sentence indicates the corresponding fields in the subscripts. It follows from Lemma 3.5 and (4.1) that for the composite map $\varphi' := \eta_F \circ \varphi \circ \eta_P^{-1}$, we have that

$$\varphi' \colon L' \to L \text{ is a 0-, 1-, and cover-preserving lattice embedding} \tag{5.4}$$

$$\text{and } \varphi'(\vec{f}') = \vec{f}, \text{ understood componentwise.} \tag{5.5}$$

First, we deal with the second inequality in (3.4). As P is a prime field, we know from Gelfand and Ponomarev's result (see also lines 2–3 of page 494 in Zádori [22] or Section 8 here) that L' is 4-generated. Pick a 4-dimensional generating vector $\vec{g}' = (g'_1, g'_2, g'_3, g'_4)$ of L' and, with φ' from (5.4), let

$$g_i := \varphi'(g'_i) \text{ for } i \in [4]; \text{ so } \varphi'(\vec{g}') = (g_1, \ldots, g_4). \tag{5.6}$$

Denote by M and m the denominator and the second summand occurring in (3.4), respectively. So $M = \lfloor d^2/4 \rfloor$ and $m = \lceil t/M \rceil$. Since $mM \geq t = f^{\mathrm{mng}}(F)$, there exist not necessarily distinct elements $r_{i,j} \in F \setminus \{0\}$, $i \in [m]$ and $j \in [M]$, such that $\{r_{i,j} : i \in [m] \text{ and } j \in [M]\}$ generates F as a field. Consider the following $\lfloor d/2 \rfloor$-by-d "pattern matrix"

$$A := \begin{pmatrix} \forall & 0 & 0 & \ldots & 0 & 0 & \forall & \ldots & \forall & -1 \\ 0 & \forall & 0 & \ldots & 0 & 0 & \forall & \ldots & \forall & -1 \\ 0 & 0 & \forall & \ldots & 0 & 0 & \forall & \ldots & \forall & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ldots & \vdots & -1 \\ 0 & 0 & 0 & \ldots & \forall & 0 & \forall & \ldots & \forall & -1 \\ 0 & 0 & 0 & \ldots & 0 & \forall & \forall & \ldots & \forall & -1 \end{pmatrix}. \tag{5.7}$$

Using (3.5), we obtain that A contains exactly M universal quantifiers. For $i \in [m]$, we obtain a "real matrix" $A(i)$ from A by changing the universals quantifiers to $r_{i,1}, \ldots, r_{i,M}$. So each of the $r_{i,1}, \ldots, r_{i,M}$ occurs in $A(i)$ exactly once and it occurs at a place where A contains a universal quantifier. Each row of $A(i)$ consists of the coordinates of a finite point of $P_{d-1} = P_{d-1}(F)$; let $\vec{u}^{(i,1)}, \ldots, \vec{u}^{(i,\lfloor d/2 \rfloor)}$ be the finite points corresponding to the rows of $A(i)$ in this way. For example, $r_{i,1}$, $\ldots$, $r_{\lceil d/2 \rceil}$ are substituted into the first row of the pattern matrix to obtain the first row of $A(i)$ and so

$$\vec{u}^{(i,1)} = [r_{i,1}, 0, 0, \ldots, 0, 0, r_{i,2}, \ldots, r_{\lceil d/2 \rceil}, -1]. \tag{5.8}$$

We often refer to the rows of $A(i)$ as points of P_{d-1}. For $i \in [m]$, let

$$g_{4+i} \text{ be the subspace of } P_{d-1} \text{ spanned by } \{\vec{u}^{(i,1)}, \ldots, \vec{u}^{(i,\lfloor d/2 \rfloor)}\}. \tag{5.9}$$

In other words, g_{4+i} is the subspace of P_{d-1} spanned by the rows of $A(i)$. For a subset X of L, let $[X]_{\mathrm{lat}}$ denote the sublattice of L that X generates; we shorten $[\{x_1, \ldots, x_n\}]_{\mathrm{lat}}$ to $[x_1, \ldots, x_n]_{\mathrm{lat}}$. Having (5.6) and (5.9), we claim that $\vec{g} := (g_1, g_2, \ldots, g_{4+m})$ is a generating vector of L, that is,

$$\text{letting } S_0 := [g_1, g_2, \ldots, g_{4+m}]_{\mathrm{lat}}, \text{ we claim that } S_0 = L. \tag{5.10}$$

Since $\{g_1, \dots, g_4\}$ generates $\varphi'(L')$, we have that $\varphi'(L') \subseteq S_0$. Thus, with reference to (4.2), (4.3), (4.4), and (5.5), we have that

$$\text{the components of } \vec{f} \text{ are in } [g_1, \dots, g_4]_{\mathrm{lat}} \subseteq S_0. \tag{5.11}$$

Let[8]

$$S_1 := [\{g_5, \dots, g_{4+m}\} \cup \{\text{the components of } \vec{f}\}]_{\mathrm{lat}}. \tag{5.12}$$

As it is clear from (5.11), to prove (5.10), it suffices to show that S_1 equals L. As a first but a long step, we show that

$$R\langle d, 1\rangle \subseteq S_1. \tag{5.13}$$

First we show that for all $i \in [m]$,

$$\text{every row of } A(i), \text{ as a point of } P_{d-1} \text{ and an atom of } L, \text{ is in } S_1. \tag{5.14}$$

By symmetry, it suffices to show that $\vec{u}^{(i,1)}$ from (5.8) is in S_1. By (5.12),

$$a_1 \vee a_{\lfloor d/2 \rfloor + 1} \vee a_{\lfloor d/2 \rfloor + 2} \vee \dots \vee \vee a_{d-1} \vee a_d \in S_1. \tag{5.15}$$

Observation 5.1, (4.3), and (4.4) imply that the subspace in (5.15) consists of the points of the form $[x_1, 0 \dots, 0, x_{\lfloor d/2 \rfloor + 1}, \dots, x_d]$ where the components are in F, not all of them is 0, and $x_d \in \{0, -1\}$. So when we form the meet of g_{4+i} and the subspace (5.15), then the fact that none of the $r_{i,j}$'s in (the "diagonal part" of) $A(i)$ is 0 and Observation 5.1 imply that this meet is $\vec{u}^{(i,1)}$. So $\vec{u}^{(i,1)} \in S_1$, proving (5.14).

Next, we show that for all $(i, j) \in [m] \times [M]$,

$$\delta_{d,1}(r_{i,j}) = [r_{i,j}, 0, \dots, 0, -1] \in S_1, \tag{5.16}$$

where $\delta_{d,1}$ is taken from Theorem 4.1. To ease the notation, we show this only for $r_{i,2}$; we can obtain the set membership $\delta(r_{i,j}) \in S_1$ for all $j \in [M]$ analogously or we can conclude it by symmetry. Letting $\iota := 1 + \lfloor d/2 \rfloor$, we know from (5.8) that $r_{i,2}$ is the ι-th coordinate of $\vec{u}^{(i,1)}$. So it follows from Observation 5.1, (4.12), and (4.3)–(4.4) that

$$\begin{aligned} \delta_{d,\iota}(r_{i,2}) &= [0, \dots, 0, r_{i,2}, 0, \dots, 0, -1] \\ &= (a_\iota \vee a_d) \wedge \Bigl(\vec{u}^{(i)} \vee \bigvee_{j \in [d-1] \setminus \{\iota\}} a_j\Bigr); \end{aligned} \tag{5.17}$$

the validity of (5.17) is also explained by Figure 1. Indeed, the figure shows how to extract the homogeneous coordinate u_ι of a finite point $\vec{u}$ in the particular case when $d = 4$ and $\iota = 3$; this technique is applicable to $\vec{u} := \vec{u}^{(i,1)}$, too. The first meetand in (5.17) is the vertical magenta coordinate axis $a_3 \vee a_4$ in the figure. The second meetand in (5.17) is the the horizontal magenta hyperplane $\vec{u} \vee a_1 \vee a_2$ through $\vec{u}$. The meet of these two meetands is $\vec{v}^{(3)} = \delta_{4,3}(u_3)$, a copy of u_ι in the coordinate ring $R\langle d, \iota\rangle$. Since $\vec{u}^{(i,1)}$ is in S_1 by (5.14) and so are the a_j's occurring in (5.17) by (5.12), we obtain that $\delta_{d,\iota}(r_{i,2}) \in S_1$. By (4.12), $\delta_{d,\iota}(r_{i,2}) \in R\langle d, \iota\rangle$. As (4.11) mentions, the ring isomorphisms given in (4.14) and (4.15) are composed from lattice operations and constants that are components of the frame $\vec{f}$ and so

[8]For *this* proof, working with S_0 would be sufficient. We introduce S_1 and later S, because S will be referenced in Section 6.

they are in S_1 by (5.12). Hence, S_1 is closed with respect to these isomorphisms, and we obtain the set membership part "$\in$" of

$$\delta_{d,1}(r_{i,2}) = F\left(\begin{smallmatrix} d & \iota \\ d & 1 \end{smallmatrix}\right)(\delta_{d,\iota}(r_{i,2})) \in S_1. \tag{5.18}$$

As the equality part follows from (4.13), so (5.18) holds. Clearly, the argument above is applicable for any $j \in [M]$, not just for $j = 2$, since we can replace $\vec{u}^{(i,1)}$ with the row of $A(i)$ that contains $r_{i,j}$. (Note that for $j = 1$ we have that $\iota = 1$ and so (4.13) is not needed.) Therefore, (5.18) holds for any $j \in [M]$, not only for $j = 2$. That is, we have proved (5.16). Applying (4.11) to the field operations (4.8), (4.9), (4.10), and (5.3), we obtain that S_1 is closed with respect to the field operations of $R\langle d, 1\rangle$. As the field isomorphism $\delta_{d,1}$ sends generating sets to generating sets, (5.16) yields that S_1 contains a generating set of the field $R\langle d, 1\rangle$. The two just-mentioned facts imply (5.13).

Next, with reference to let (4.2)–(4.4), let

$$S := [\{\text{the components of the canonical frame}\} \cup R\langle d, 1\rangle]_{\text{lat}}. \tag{5.19}$$

We obtain from (5.12) and (5.13) that $S \subseteq S_1$. Therefore, to prove that $S_1 = L$ and so (5.10) holds, it suffices to show that

$$S, \text{ defined in (5.19), equals } L = \text{Sub}(P_{d-1}). \tag{5.20}$$

For later reference, we note that our argument

$$\text{proving (5.20) does not use Gelfand and Ponomarev's theorem,} \tag{5.21}$$

which has already been mentioned; see also Theorem 8.1 in Section 8.

Next, we aim to prove (5.20). From (4.11), we know that S is closed with respect to the ring isomorphisms in (4.14) and (4.15). Thus, for any $i, j \in [d]$ such that $i \neq j$ and for any $r \in F$,

$$R\langle i, j\rangle \subseteq S \text{ and so } [0, \ldots, 0, 1, 0, \ldots, 0, -1, 0, \ldots, 0] \in S, \tag{5.22}$$

where r and -1 are at the j-th position and the i-th positions, respectively. Since each element of L is the join of finitely many atoms, it suffices to show that any projective point $\vec{u} = [u_1, \ldots, u_d]$ belongs to S. Since at least one of the homogeneous coordinates $u_1, \ldots, u_d$ is nonzero, symmetry allows us to assume that $u_d \neq 0$. That is, by homogeneity, we assume that $u_d = -1$. Letting $\vec{v}^{(i)} = [0, \ldots, 0, u_i, 0, \ldots, 0, -1]$ (where u_i is sitting in the i-th component) for $i \in [d-1]$, we have that $\vec{v}^{(i)} \in R\langle d, i\rangle \subseteq S$ by (5.22). Figure 1 visualizes the situation for $d = 4$. In the figure, the black-filled elements are in S by (5.19) and (5.22), and therefore so are the three depicted hyperplanes containing the empty-filled $\vec{u}$. Among these three hyperplanes, one is adorned in green, another in magenta, and the third is filled with a floral pattern. (When translated to grayscale, the green plane appears lighter than its magenta counterpart.) As $\vec{u}$ is the meet of the three hyperplanes, $\vec{u} \in S$ is clear when $d = 4$. The same idea works for any $3 \leq d \in \mathbb{N}^+$; indeed,

$$\vec{u} := \bigwedge_{i=1}^{d-1} \Big(\vec{v}^{(i)} \vee \bigvee_{j \in [d-1] \setminus \{i\}} a_j \Big) \in S$$

follows in a straightforward way by using Observation 5.1. Thus, (5.20) holds, implying (5.10) and the second inequality in (3.4).

Our argument to show the first inequality in (3.4) is practically the same as that of Strietz [17] for partition lattices[9]. The key is Wille's D_2 Lemma:

Lemma 5.3 (D_2-Lemma in Wille [21])**.** *If a subdirectly irreducible modular lattice with more than two elements is generated by $e_0, e_1, \ldots, e_t$, then $e_0 \vee \cdots \vee e_{i-1} \geq e_i \wedge \cdots \wedge e_t$ for every $i \in [t]$.*

By (4.1), $L \cong \mathrm{Sub}({}_FV)$, where $V = {}_FF^d$. We know from the folklore that $\mathrm{Sub}({}_FV)$ is subdirectly irreducible. Having no reference to this fact at hand, we present an easy in-line proof here; some details of this proof will also be used later. Let a and b be distinct atoms of $\mathrm{Sub}({}_FV)$, then $a = F\vec{w}^{(1)}$ and $b = F\vec{w}^{(2)}$ with the uniquely determined and linearly independent vectors $\vec{w}^{(1)} = (w_1^{(1)}, \ldots, w_d^{(1)})$ and $\vec{w}^{(2)} = (w_1^{(2)}, \ldots, w_d^{(2)})$ in V such that $w_1^{(1)} + \cdots + w_d^{(1)} = 1$ and $w_1^{(2)} + \cdots + w_d^{(2)} = 1$. Letting $c := F(\vec{w}^{(1)} + \vec{w}^{(2)})$, a trivial computation shows that $\{0 = a \wedge b, a, b, c, a \vee b\}$ is a sublattice isomorphic to M_3, the 5-element modular lattice of length 2. Therefore, the (clearly) atomistic and modular lattice $\mathrm{Sub}({}_FV)$ is subdirectly irreducible by lines 4–5 in page 349 of Grätzer [8]. For later reference, let us summarize what we have also obtained:

Observation 5.4. *For any two distinct atoms a and b of $\mathrm{Sub}({}_FV)$, c defined above by $c := F(\vec{w}^{(1)} + \vec{w}^{(2)})$ is a third atom, $\{0, a, b, c, a \vee b\}$ is a sublattice of $\mathrm{Sub}({}_FV)$, and this sublattice is isomorphic to M_3.*

Returning to the proof of Theorem 3.1, let us assume, to reach a contradiction, that $L = \mathrm{Sub}({}_FV)$ is generated by a subset $\{e_0, e_1, e_2\}$. Applying Lemma 5.3, we have that $e_0 \geq e_1 \wedge e_2$ and $e_0 \vee e_1 \geq e_2$. These two inequalities and those that we obtain from them by permuting the generators imply that $\{e_0, e_1, e_2\}$ generates an M_3 sublattice, which is a contradiction showing that $f^{\mathrm{mng}}(L) \geq 4$. We have verified both inequalities in (3.4), and the proof of Theorem 3.1 is complete. □

6. Proving Theorem 3.2

As a preparation for the proof of the second theorem, we prove the following easy lemma.

Lemma 6.1. *Assume that $L_1, \ldots, L_k$ are finitely generated lattices, $L = L_1 \times \cdots \times L_k$ is their direct product, and $\vec{b}^{(1)} = (b_1^{(1)}, \ldots, b_k^{(1)})$, …, $\vec{b}^{(t)} = (b_1^{(t)}, \ldots, b_k^{(t)})$ are elements of L. Then $\{\vec{b}^{(1)}, \ldots, \vec{b}^{(t)}\}$ generates L if and only if*

(1) For each $i \in [k]$, $\{b_i^{(1)}, \ldots, b_i^{(t)}\}$ generates L_i, and

(2) For each $i \in [k]$, there is a t-ary lattice term f_i such that $f_i(b_i^{(1)}, \ldots, b_i^{(t)})$ equals 1_i, the top element of L_i, but for every $j \in [k] \setminus \{i\}$, $f_i(b_j^{(1)}, \ldots, b_j^{(t)})$ equals 0_j, the bottom element of L_j.

Visually, we can form a k-by-t matrix with the $\vec{b}^{(i)}$'s being the columns and we apply the terms f_i to the rows of this matrix.

Proof. First of all, note that 1_i and 0_j in the lemma exist since L_i and L_j are finitely generated. To prove the "only if" part, assume that $\{\vec{b}^{(1)}, \ldots, \vec{b}^{(t)}\}$ generates L.

[9]As partition lattices with more than five elements are not modular, we note that Lemma 5.3, quoted from Wille [21], is valid even without assuming modularity. Lemma 4.1 from Czédli [2], a variant of the D_2-Lemma, would also suffice here.

Since the i-th projection $L \to L_i$ defined by $(x_1, \ldots, x_k) \mapsto x_i$ sends generating sets to generating sets, (1) holds. So does (2) since there is a lattice term f_i such that $(0, \ldots, 0, 1, 0, \ldots, 0) \in L$ (with 1 sitting at the i-th place) equals $f_i(\vec{b}^{(1)}, \ldots, \vec{b}^{(t)})$.

To prove the "if" part, assume that (1) and (2) hold, and let $\vec{w} = (w_1, \ldots, w_k) \in L$. For each $i \in [k]$, (1) allows us to pick a t-ary lattice term g_i such that $g_i(b_i^{(1)}, \ldots, b_i^{(t)}) = w_i$ in L_i. Furthermore, (2) yields a t-ary lattice term f_i such that $f_i(b_i^{(1)}, \ldots, b_i^{(t)}) = 1_i$ but $f_i(b_j^{(1)}, \ldots, b_j^{(t)}) = 0_j$ for all $j \in [k] \setminus \{i\}$. Then

$$\vec{w} = \bigvee_{i \in [k]} \bigl(g_i(\vec{b}^{(1)}, \ldots, \vec{b}^{(t)}) \wedge f_i(\vec{b}^{(1)}, \ldots, \vec{b}^{(t)})\bigr) \in [\vec{b}^{(1)}, \ldots, \vec{b}^{(t)}]_{\mathrm{lat}}$$

completes the proof of Lemma 6.1. □

The following well-known fact follows from, say, Vanstone and Oorschot [18, Theorem 3.3].

Fact 6.2. For $d \in \mathbb{N}^+$ and a field F, $\mathrm{Sub}({}_F F^d)$ is a selfdual lattice.

Proof of Theorem 3.2. To ease the notation, let $h := \lfloor d/2 \rfloor$ ("h" comes from half) and $r := 4 + \lceil t/\lfloor d^2/4 \rfloor \rceil$. We know from (3.4) in Theorem 3.1 that $L = \mathrm{Sub}({}_F V)$ has an r-dimensional generating vector.

First, we show (3.8). By Remark 3.4, it suffices to show that L^μ is $(1 + r)$-generated. For $i \in \{1, h\}$, let A_i be the set of i-dimensional subspaces of V, that is, A_i is the set of elements of height i in L. In particular, A_1 is the set of atoms of L and $|A_h| = \mu$; see (3.6). Define a binary operation "product" on A_1 as follows: For $a, b \in A_1$, let

$$ab := \begin{cases} c \text{ defined in Observation 5.4} & \text{if } a \neq b \text{ and} \\ 0 = 0_L & \text{if } a = b. \end{cases} \tag{6.1}$$

This operation, denoted by concatenation, has precedence over the lattice operations. Clearly, Observation 5.4 implies the following.

Fact 6.3. For any $b, e \in A_1$, either $b \neq e$ and $\{0, b, be, e, be \vee e\}$ is a sublattice isomorphic to M_3, or $b = e$ and $be = 0$; in both cases, $b \leq be \vee e$.

Let $\vec{g} = (g_1, \ldots, g_r)$ be a generating vector of L. Let $u_1, \ldots, u_\mu$ be a repetition-free enumeration of the elements of (the μ-element) A_h. For $j \in [r]$, we define $\vec{b}^{(j)} \in L^\mu$ as the constant vector $(g_j, g_j, \ldots, g_j)$. We define a further vector, $\vec{b}^{(0)} := (u_1, u_2, \ldots, u_\mu) \in L^\mu$. We claim that

$$\Psi := \{\vec{b}^{(0)}, \vec{b}^{(1)}, \ldots, \vec{b}^{(r)}\} \text{ generates } L^\mu. \tag{6.2}$$

Since $[u_i, g_1, \ldots, g_r]_{\mathrm{lat}} = L$ for all $i \in [\mu]$, Ψ (apart from self-explanatory notational differences) satisfies (1) of Lemma 6.1.

Showing that Ψ satisfies (2) of Lemma 6.1, too, needs more work. For each $i \in [\mu]$, fix an h-element subset S_i of A_1 such that $u_i = \bigvee\{e : e \in S_i\}$. Let $\vec{\xi} = (\xi_1, \ldots, \xi_r)$ be a vector of variables, and let $\vec{\xi}^+$ stand for $(\xi_0, \xi_1, \ldots, \xi_r)$. For each element w of L, let us fix an r-ary lattice term $w^*(\vec{\xi})$ such that $w^*(\vec{g}) = w$. If $w = ab$, see (6.1), then $w^*(\vec{\xi})$ is written as $(ab)^*(\vec{\xi})$. We can fix a d-element subset B of A_1 such that $1 = 1_L$ equals $\bigvee B$. For each $i \in [\mu]$, we define the following

lattice term:

$$f_i(\vec{\xi}^+) := \bigvee_{b\in B}\Bigl(b^*(\vec{\xi}) \wedge \bigwedge_{e\in S_i}\Bigl((be)^*(\vec{\xi}) \vee \bigl(\xi_0 \wedge e^*(\vec{\xi})\bigr)\Bigr)\Bigr). \tag{6.3}$$

Let $(u_j, \vec{g}) := (u_j, g_1, \ldots, g_r)$. We need to show that $f_i(u_j, \vec{g}) = 0_L$ if $j \neq i$ and it is 1_L if $j = i$. For the meetand $\beta_{b,e}(\vec{\xi}^+) := (be)^*(\vec{\xi}) \vee \bigl(\xi_0 \wedge e^*(\vec{\xi})\bigr)$ occurring in (6.3),

$$\beta_{b,e}(u_j, \vec{g}) = (be)^*(\vec{g}) \vee \bigl(u_j \wedge e^*(\vec{g})\bigr) = be \vee \bigl(u_j \wedge e\bigr). \tag{6.4}$$

There are two cases to consider. First, assume that $j = i$. Then, for every $e \in S_i = S_j$, $e \leq u_j$ yields that $\beta_{b,e}(u_j, \vec{g}) = be \vee e$, whereby Fact 6.3 implies that $b^*(\vec{g}) = b \leq \beta_{b,e}(u_j, \vec{g})$. Thus, the meet $\bigwedge_{e\in S_i}$ as a meetand in (6.3) makes no effect and we obtain that $f_i(u_j, \vec{g}) = \bigvee_{b\in B} b^*(\vec{g}) = \bigvee_{b\in B} b = 1_L$ if $j = i$, as required.

Second, assume that $j \neq i$. Since $u_i = \bigvee S_i$ and u_j, belonging to the antichain A_h, are incomparable, there is an $e \in S_i$ such that $e \not\leq u_j$. For this atom e, $u_j \wedge e$ in (6.4) is 0_L, whence $\beta_{b,e}(u_j, \vec{g}) = be$. Thus, each of the joinands of $\bigvee_{b\in B}$ in (6.3) is (at most) $b^*(\vec{g}) \wedge \beta_{b,e}(u_j, \vec{g}) = b \wedge be = 0$, no matter whether $b = e$ or $b \neq e$. Therefore, $f_i(u_j, \vec{g}) = 0$ if $j \neq i$, as required. Hence, Ψ satisfies (2) of Lemma 6.1, whereby we conclude (6.2). Thus, $f^{\mathrm{mng}}(L^k) \leq f^{\mathrm{mng}}(L^\mu) \leq 1 + r = 5 + \lceil t/\lfloor d^2/4\rfloor\rceil$, proving (3.8).

Next, we deal with the first equality in (3.7). Let $M := \lfloor d^2/4\rfloor$ and $m := f^{\mathrm{mng}}(L)$. For the sake of contradiction, suppose that

$$m = f^{\mathrm{mng}}(L) < \lceil t/M\rceil \quad \text{(indirect assumption)}. \tag{6.5}$$

Let $\{g_1, \ldots, g_m\}$ be a generating set of $L = \mathrm{Sub}(V) = \mathrm{Sub}({}_FF^d)$. For each $i \in [m]$, let n_i be the dimension of the subspace g_i. Let us pick an n_i-by-d matrix $B(i)$ over F such that the rows of $B(i)$ form a basis of g_i. After performing the Gauss–Jordan elimination to the rows of $B(i)$, these rows still form a basis of g_i. Hence, we can assume that $B(i)$ is in reduced row echelon form and the number n_i of its rows equals its rank. So for $j, \iota \in [n_i]$, the ι-th element in the j-th row of $B(i)$ is $\delta_{j,\iota}$ (Kronecker delta). Note that $B(i)$ has the same shape as $A(i)$ in (5.7) would have if we changed the universal quantifiers in the main diagonal to units (that is, to 1's). Let $H(i)$ stand for the set of those entries of $B(i)$ that differ from 0 and 1. This entries are in the last $d - n_i$ columns, so $|H(i)| \leq n_i(d - n_i)$. Hence, using (3.5) and that the quadratic function $x \mapsto x(d - x)$ takes its maximum at $d/2$, it follows that $|H_i| \leq n_i(d - n_i) \leq M$. Letting $H := H(1) \cup \cdots \cup H(m)$, we have that $|H| \leq mM$. Observe that no matter whether t/M is an infinite cardinal, an integer number, or a non-integer number, the indirect assumption (6.5) and $m \in \mathbb{N}_0$ imply that

$$m < t/M, \text{ whereby } |H| \leq mM < t = f^{\mathrm{mng}}(F). \tag{6.6}$$

Let P denote the subfield of F generated by H. By (6.6), $P \subset F$ (proper subfield). With $V' := {}_PP^d$ and $L' := \mathrm{Sub}({}_PV')$, φ from Lemma 3.5 is a lattice embedding $L' \to L$. For $i \in [m]$, using that $B(i)$ is also a matrix over P, let g'_i be the subspace of V' spanned by the rows of $B(i)$. Denoting the set of rows of $B(i)$ by $X^{(i)}$, the last sentence of Lemma 3.5 gives that

$$\varphi(g'_i) = \varphi(\mathrm{Span}_P(X^{(i)})) = \mathrm{Span}_F(X^{(i)}) = g_i \tag{6.7}$$

for $i \in [m]$. Since φ is an embedding, $\varphi(L')$ is a sublattice of L. This sublattice includes the generating set $\{g_i : i \in [m]\}$ by (6.7). Thus, $\varphi(L') = L$, implying

that φ is surjective. Pick an element $r \in F \setminus P$. By the surjectivity of φ, the 1-dimensional subspace $S := \mathrm{Span}_F(\{(r, 1, 1, \ldots, 1)\}) \in L$ has a φ-preimage $S' \in L$. Since φ is length-preserving by Lemma 3.5, S' is also 1-dimensional. So $S' := \mathrm{Span}_P(\{(p, q_2, q_3, \ldots, q_d)\})$ for some $p, q_2, \ldots, q_d \in P$. The last sentence of Lemma 3.5 yields a $\lambda \in F$ such that $(r, 1, 1, \ldots, 1) = \lambda(p, q_2, q_3, \ldots, q_d)$. Comparing the second components, $\lambda = q_2^{-1} \in P$. Thus, the equality of the first components yields that $r = p\lambda \in P$, contradicting the choice of r. Now that the indirect assumption (6.5) has lead to a contradiction, we have shown the first inequality in (3.7). Remark 3.4 gives the second inequality, so we have proved (3.7).

The components of $\vec{g}$: 

The generated sublattice $\setminus \{0, 1\}$ is only: 

FIGURE 3. For $\vec{g} = \vec{g}^{(i)}$, $\mathrm{typ}(\vec{g})$ cannot be $(2, 2)$

Next, we turn our attention to (3.9) and (3.10). So we assume that F is a prime field and $d = 2$. Furthermore, based on the isomorphism given in (4.1), let $P_{d-1} = P_2 = P_2(F)$ be the projective plane over F and, in the rest of the proof of Theorem 3.2, let $L := \mathrm{Sub}(P_2)$. Some geometric terms and methods in addition to the lattice theoretic ones will frequently appear in our considerations. In particular, instead of drawing a usual Hasse diagram of $L = \mathrm{Sub}(P_2)$, we visualize L and its sublattices by drawing the points and lines they contain. Furthermore, we frequently use the following definition (but only for projective *planes*) without referencing it.

Definition 6.4. For $L = \mathrm{Sub}(P_2)$ and a quadruple $\vec{g} = (g_1, \ldots, g_4) \in L^4$, we say that $\vec{g}$ is in *general position* if for any $\{i, j, k\} \subset [4]$ such that $|\{i, j, k\}| = 3$,

- $g_i \not\leq g_j$, that is, $\{g_1, \ldots, g_4\}$ is an antichain;
- if g_i, g_j, and g_k are points, then $g_i \not\leq g_j \vee g_k$, that is, no three collinear points occur among the components of $\vec{g}$; and
- if g_i, g_j, and g_k are lines, then $g_j \wedge g_j \not\leq g_k$, that is, no three concurrent lines occur among the components of $\vec{g}$.

A *complete quadrangle* is a quadruple $\vec{g} = (g_1, \ldots, g_4)$ in general position such that $g_1, \ldots, g_4$ are points.

Analogously to an earlier notation, A_1 is the set of points while A_2 is the set of lines. We show that

$$\text{if } t = 0,\ d = 3, \text{ and } f^{\mathrm{mng}}(L^k) = 4, \text{ then } k \leq 4. \tag{6.8}$$

So F is a prime field now, and we can assume that k is the largest positive integer such that $f^{\mathrm{mng}}(L^k) = 4$. This makes sense since $k \geq 1$ by (3.4) and the maximum exists by Observation 2.1. Choose a 4-dimensional generating vector $(\vec{b}^{(1)}, \ldots, \vec{b}^{(4)})$ of L^k. (Here the $\vec{b}^{(i)}$, $i \in [4]$, are also vectors since they belong to L^k.) Let

$$\vec{g}^{(i)} = (g_1^{(i)}, g_2^{(i)}, g_3^{(i)}, g_4^{(i)}) := (b_i^{(1)}, b_i^{(2)}, b_i^{(3)}, b_i^{(4)}) \text{ for } i \in [k];$$
$$\text{it is a generating vector of } L \text{ by Lemma 6.1.} \tag{6.9}$$

Define the *Kronecker delta* in a lattice L by $\delta_{ii}^{(L)} := 1_L$ and, for $j \neq i$, $\delta_{ij}^{(L)} := 0_L$. Let f_i, $i \in [k]$, be the quaternary lattice terms provided by Lemma 6.1; then

$$f_i(\vec{g}^{(j)}) = \delta_{ij}^{(L)}. \tag{6.10}$$

As $\{g_1^{(i)}, \ldots, g_4^{(i)}\}$ generates L, it is easy to see that for each $i \in [k]$ and $j \in [4]$, $g_j^{(i)}$ is a point or a line. For later reference, we formulate this fact:

$$g_j^{(i)} \notin \{0, 1\} \text{ and any 4-element generating set} \subseteq A_1 \cup A_2. \tag{6.11}$$

The components of $\vec{g}$:  The generated sublattice $\setminus \{0, 1\}$ is only: 

FIGURE 4. A quadruple of points not in general position

For $x \in L$, let $\operatorname{hgh}(x)$ denote the *height* of x; it is the projective dimension plus 1. For example, for $x \in A_1$, $\operatorname{hgh}(x) = 1$. For a generating vector $\vec{g} = (g_1, g_2, g_3, g_4) \in L^4$ of L, define the *type* and the *fine type* of $\vec{g}$ as

$$\operatorname{typ}(\vec{g}) := (|\{i \in [4] : g_i \text{ is a point}\}|, |\{i \in [4] : g_i \text{ is a line}\}|) \text{ and}$$
$$\operatorname{ftyp}(\vec{g}) := (\operatorname{hgh}(g_1), \operatorname{hgh}(g_2), \operatorname{hgh}(g_3), \operatorname{hgh}(g_4)).$$

We know from (6.11) that the sum of the components of $\operatorname{typ}(\vec{g})$ and that of $\operatorname{ftyp}(\vec{g})$ are 4. It follows from (6.9) and (6.11) that for every generating quadruple $\vec{h}$ and, in particular, for every $i \in [k]$

$$\operatorname{ftyp}(\vec{h}) \in \{1, 2\}^4 \text{ and } \operatorname{ftyp}(\vec{g}^{(i)}) \in \{1, 2\}^4. \tag{6.12}$$

The *type of a fine type* $\vec{\tau} \in \{1, 2\}^4$ is $\operatorname{typ}(\vec{\tau}) := (|\{i \in [4] : \tau_i = 1\}|, |\{i \in [4] : \tau_i = 2\}|)$. Note the obvious rule: $\operatorname{typ}(\operatorname{ftyp}(\vec{g}^{(i)})) = \operatorname{typ}(\vec{g}^{(i)})$ for every $i \in [k]$. Note also that our figures and arguments

$$\text{will omit the most trivial cases like } g_1^{(i)} = g_2^{(i)}. \tag{6.13}$$

Using that every line contains at least three points, Figure 3 shows that for any generating quadruple $\vec{h}$ and, in particular, for $i \in [k]$,

$$\text{neither } \operatorname{typ}(\vec{h}) \text{ nor } \operatorname{typ}(\vec{g}^{(i)}) \text{ can be } (2, 2). \tag{6.14}$$

In P_2, any two distinct lines intersect in a point. The following fact is also well known; see, for example, Veblen and Young [19, page 93].

Fact 6.5. If $\vec{x} = (x_1, \ldots, x_4)$ and $\vec{x}' = (x_1', \ldots, x_4')$ are complete quadrangles in P_2, then P_2 has an automorphism φ such that $\varphi(x_i) = x_i'$ for $i \in [4]$. Consequently, L also has such an automorphism.

Therefore, our figures are sufficiently general. We claim the following.

Fact 6.6. Every generating quadruple of L is in general position.

To show this, assume that $\vec{h}$ is a generating quadruple. Since $\operatorname{typ}(\vec{h}) \neq (2, 2)$ by (6.14) and L is selfdual, see Fact 6.2, we can assume that $\operatorname{typ}(\vec{h}) \in \{(4, 0), (3, 1)\}$. If $\operatorname{typ}(\vec{h}) = (4, 0)$, then $\vec{h}$ is in general position by Figure 4 and (6.13). For $\operatorname{typ}(\vec{h}) = (3, 1)$, we draw the same conclusion from Case 1 of Figure 5 and Figure 6. Thus, Fact 6.6 holds.

Our next step is to show the following fact.

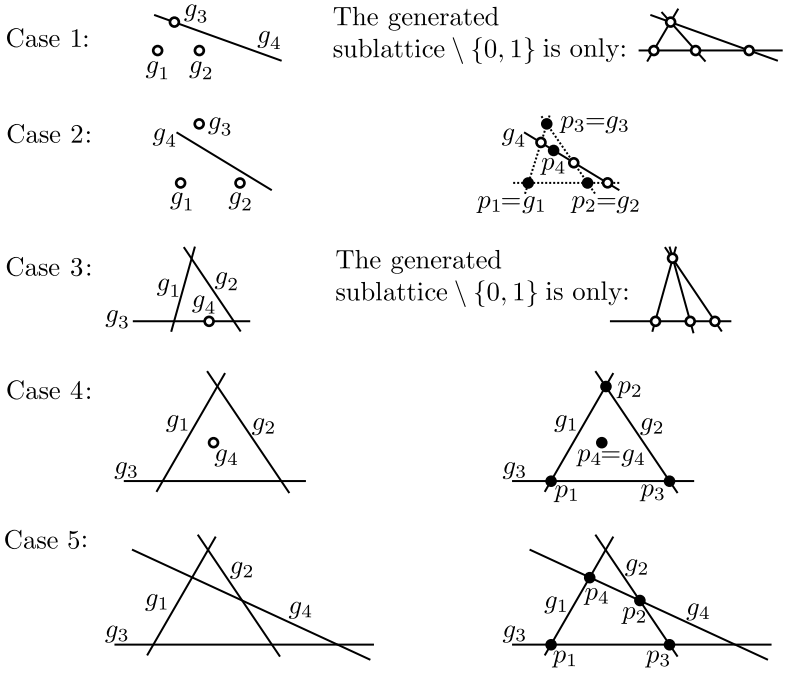

FIGURE 5. Proving Fact 6.7

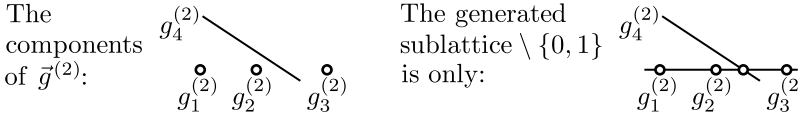

FIGURE 6. Three collinear points and a line

Fact 6.7. If $|F| \geq 3$, then for each generating vector $\vec{g} = (g_1, g_2, g_3, g_4)$ of L, there is a complete quadrangle $(p_1, \ldots, p_4)$ of L such that $p_i \leq g_i$ for $i \in [4]$.

To show Fact 6.7, observe that Facts 6.5 and 6.6 take care of the case $\operatorname{typ}(\vec{g}') = (4, 0)$. Hence, there are five cases to consider, see Figure 5, but each of them is obvious. We exclude Cases 1 and 3 since then $\{g_1, \ldots, g_4\}$ does not generate L; indeed, the figure shows on the right what the generated sublattice is and this sublattice is clearly not the whole L since every line of the projective plane has at least three[10] points. In Cases 2, 4, and 5, the figure shows how to choose the p_i's. Note for later reference that only Case 2 needs the assumption that $|F| \geq 3$, which makes it possible to pick a fourth point on the line g_4. So, Figure 5 has proved Fact 6.7.

Now we can show that

$$\text{if } \operatorname{typ}(\vec{g}^{(i)}) \in \{(4, 0), (0, 4)\} \text{ for some } i \in [k], \text{ then } k = 1. \tag{6.15}$$

[10]We now have at least four points since $|F| \geq 3$. However, we continue to use the term "at least three points" to make this argument applicable also when $|F| = 2$.

For the sake of contradiction, suppose that, say, $\operatorname{typ}(\vec{g}^{(1)}) \in \{(4,0),(0,4)\}$ but $k > 1$. By the selfduality of L, see Fact 6.2, we can assume that $\operatorname{typ}(\vec{g}^{(1)}) = (4,0)$. First, we assume that $|F| \geq 3$. Fact 6.7 yields a complete quadrangle $\vec{p}$ such that $p_i \leq g_i^{(2)}$ for $i \in [4]$. By Fact 6.6, $\vec{g}^{(1)}$ is a complete quadrangle. Thus, by Fact 6.5, we can take an automorphism φ of L such that $\varphi(\vec{g}_i^{(1)}) = p_i \leq g_i^{(2)}$ for $i \in [4]$; we write $\varphi(\vec{g}^{(1)}) \leq \vec{g}^{(2)}$ for short. Using (6.10) and the fact that f_1 is order-preserving, we obtain that

$$1 = \varphi(\delta_{11}^{(L)}) = \varphi(f_1(\vec{g}^{(1)})) = f_1(\varphi(\vec{g}^{(1)})) \leq f_1(\vec{g}^{(2)}) = \delta_{12}^{(L)} = 0, \tag{6.16}$$

which is a contradiction showing (6.15) for the case $|F| \geq 3$.

If $|F| = 2$ and so the projective plane is the Fano plane, then the argument for (6.15) needs the following modifications. Even though Case 2 of Figure 5 and Fact 6.7 fail for the Fano plane, Fact 6.7 still holds for the particular case $\operatorname{typ}(\vec{g}) \in \{(1,3),(0,4)\}$ since then the earlier argument relies only on Cases 3, 4, and 5 of Figure 5. Like we did right after (6.15), we assume that (6.15) is false and its failure is witnessed by $\vec{g}^{(1)}$ of type $(4,0)$ and $\vec{g}^{(2)}$. If $\operatorname{typ}(\vec{g}^{(2)}) \in \{(1,3),(0,4)\}$, then the just-mentioned particular case of Fact 6.7 leads to a contradiction in the same way as before. We know from (6.14) that $\operatorname{typ}(\vec{g}^{(2)}) \neq (2,2)$. If $\operatorname{typ}(\vec{g}^{(2)}) = (4,0)$, then Facts 6.5 and 6.6 give an automorphism $\varphi\colon L \to L$ such that $\vec{g}^{(2)} = \varphi(\vec{g}^{(1)})$, whereby (6.16) (with equality in its middle rather than an inequality) leads to a contradiction. Hence, based on (6.11), we can assume that $\operatorname{typ}(\vec{g}^{(2)}) = (3,1)$. Since, for any $i,j \in [k]$, $\delta_{ij}^{(L)}$ is a fixed point of every automorphism of L, it follows that for any system $(f_i : i \in [k])$ of quaternary lattice terms and for any family $(\psi_{i,j} : i,j \in [k])$ of automorphisms of L,

$$\text{(6.10) holds if an only if } f_i\big(\psi_{i,j}(\vec{g}^{(j)})\big) = \delta_{ij}^{(L)} \text{ for all } i,j \in [k]. \tag{6.17}$$

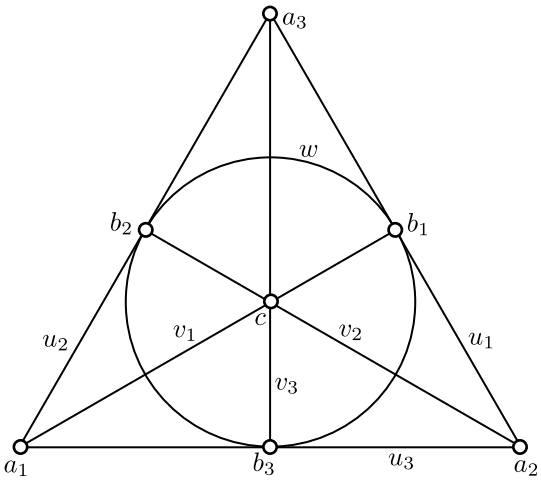

FIGURE 7. Notations for the Fano plane

Figure 7 shows how we denote the points and the lines of the Fano plane; they belong to L and $|L| = 16$. By Fact 6.6, $\vec{g}^{(2)}$ is in general position. Thus, by symmetry and (6.17), we can assume that $\vec{g}^{(2)} = (a_1, a_2, a_3, w)$; see Figure 7. By

Fact 6.5 and (6.17), we can also assume that $\vec{g}^{(1)} = (a_1, a_2, a_3, c)$. To define a subset S, let us agree that sets of the forms $\{x_i : i \in [3]\}$ and $\{x_{i,j} : i, j \in [3], i \neq j\}$ will simply be denoted by $\{x_i\}$ and $\{x_{i,j}\}$, respectively. These sets consist of three and six elements, respectively. With these temporary notations, we let

$$\begin{aligned} S := {} & \underline{\{(a_i, a_i)\}} \cup \{(u_i, u_i)\} \cup \{(b_i, u_i)\} \cup \{(0, a_i)\} \\ & \cup \{(0, b_i)\} \cup \{(0, u_i)\} \cup \{(0, v_i)\} \cup \{(a_i, 1)\} \cup \{(b_i, 1)\} \\ & \cup \{(u_i, 1)\} \cup \{(v_i, 1)\} \cup \{(a_i, v_i)\} \cup \{(a_i, u_j)\} \\ & \cup \{\underline{(c, w)}, (0, 0), (1, 1), (c, 1), (0, w), (w, 1), (0, 1), (0, c)\}; \end{aligned} \tag{6.18}$$

the underlined terms of (6.18) will occur in (6.19). It is straightforward to check[11] that S is a sublattice of L^2. This fact and (6.10) imply that

$$\begin{aligned} (1, 0) &= \bigl(\delta_{11}^{(L)}, \delta_{12}^{(L)}\bigr) = \bigl(f_1(\vec{g}^{(1)}), f_1(\vec{g}^{(2)})\bigr) \\ &= \bigl(f_1(a_1, a_2, a_3, c),\ f_1(a_1, a_2, a_3, w)\bigr) \\ &= \bigl(f_1(a_1, a_1), f_1(a_2, a_2), f_1(a_3, a_3), f_1(c, w)\bigr) \in S, \end{aligned} \tag{6.19}$$

which contradicts (6.18). Hence, (6.15) holds even if $|F| = 2$, that is, it holds for all prime fields.

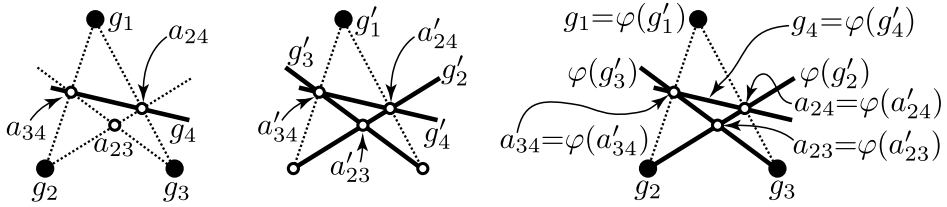

FIGURE 8. Proving Fact 6.8

Next, for fine types $(\xi_1, \xi_2, \xi_3, \xi_4)$ and $(\eta_1, \eta_2, \eta_3, \eta_4)$, let us say that they are *complementary* if $\xi_i + \eta_i = 3$ for all $i \in [4]$. (6.12) sheds more light on this concept.

Fact 6.8. If there are $\vec{g}, \vec{g}' \in \{\vec{g}^{(i)} : i \in [k]\}$ such that $\operatorname{typ}(\vec{g}) = (3, 1)$ and $\operatorname{typ}(\vec{g}') = (1, 3)$, then $k = 2$ and, furthermore, $\operatorname{ftyp}(\vec{g})$ and $\operatorname{ftyp}(\vec{g}')$ are complementary.

To show Fact 6.8 by way of contradiction, assume that $\vec{g}, \vec{g}' \in \{\vec{g}^{(i)} : i \in [k]\} =: \Gamma$ such that $\operatorname{typ}(\vec{g}) = (3, 1)$ and $\operatorname{typ}(\vec{g}') = (1, 3)$ but $\operatorname{ftyp}(\vec{g})$ and $\operatorname{ftyp}(\vec{g}')$ are not complementary. We know from Fact 6.6 that $\vec{g}$ and $\vec{g}'$ are in general position. Apart from permutations, $\operatorname{ftyp}(\vec{g}) = (1, 1, 1, 2)$ and $\operatorname{ftyp}(\vec{g}') = (1, 2, 2, 2)$; see Figure 8. The left of Figure 8 shows how to define three auxiliary points; for example (in the language of L), $a_{24} := (g_1 \vee g_3) \wedge g_4$ and $a_{23} := (a_{34} \vee g_3) \wedge (a_{24} \vee g_2)$; similarly for the middle of the figure. It is straightforward to see that if $(g_1, a_{23}, a_{24}, a_{34})$ was not in general position then neither $\vec{g}$ would be, and similarly for $(g'_1, a'_{23}, a'_{24}, a'_{34})$ in the middle of Figure 8. Hence, Fact 6.5 yields an automorphism φ of L such that $\varphi(g'_1) = g_1$, $\varphi(a'_{23}) = a_{23}$, $\varphi(a'_{24}) = a_{24}$, and $\varphi(a'_{34}) = a_{34}$; see on the right of Figure 8. As the figure shows, $\vec{g} \leq \varphi(\vec{g}')$, understood componentwise. In other words, $\varphi^{-1}(\vec{g}) \leq \vec{g}'$. As $\vec{g}$ and $\vec{g}'$ are in $\Gamma = \{\vec{g}^{(i)} : i \in [4]\}$, we can assume that

[11] Alternatively, an appropriate program in Maple V (version 5.9, 1997, Waterloo Maple Inc.) is presented in (the Appendix) Section 9; it is also is available from the author's website http://tinyurl.com/g-czedli/ .

$\vec{g}^{(1)} = \vec{g}$ and $\vec{g}^{(2)} = \vec{g}'$. So $\varphi^{-1}(\vec{g}^{(1)}) \leq \vec{g}^{(2)}$. Hence (6.16), with φ^{-1} instead of φ, gives contradiction. This shows that

$$\text{ftyp}(\vec{g}) \text{ and } \text{ftyp}(\vec{g}') \text{ are complementary, as required.} \tag{6.20}$$

Next, we show that for any fine type $\vec{\tau}$,

$$\text{there is at most one } \vec{h} \in \Gamma \text{ such that } \vec{\tau} = \text{ftyp}(\vec{h}). \tag{6.21}$$

To verify (6.21), we can assume that $\text{typ}(\tau) \neq (2,2)$ since otherwise (6.21) is clear by (6.14). So let $\vec{h}, \vec{h}' \in \Gamma$ such that $\vec{\tau} = \text{ftyp}(\vec{h}) = \text{ftyp}(\vec{h}')$; we need to show that $\vec{h} = \vec{h}'$. If $\vec{\tau} \in \{(4,0),(0,4)\}$, then $\vec{h} = \vec{h}'$ is clear by (6.15). Out of the cases $\text{typ}(\tau) = (3,1)$ and $\text{typ}(\tau) = (1,3)$, it suffices to settle the first one since then the other follows by duality; see Fact 6.2. As the components of $\vec{\tau}$ share a symmetrical role, we can assume that $\vec{\tau} = \text{ftyp}(\vec{h}) = (1,1,1,3)$; see Case 2 in Figure 5 with $\vec{g}$ instead of $\vec{h}$. No problem if $|F| = 2$, as p_4 (the fourth point on g_4) is not needed here. On the right of Case 2 in the figure, the bottom left black-filled point, the bottom right black-filled point, the middle empty-filled point, and the top left empty-filled point, in this order, form a complete quadrangle $\vec{z}$. Indeed, if $\vec{z}$ was not in general position, then neither $\vec{h}$ would be and so $\vec{h}$ would contradict Fact 6.6. Observe that $\vec{z}$ determines $\vec{h}$. Hence, applying Fact 6.5 to $\vec{z}$ and to the analogously defined quadruple determining $\vec{h}'$, Fact 6.5 implies that $\vec{h}' = \varphi(\vec{h})$ for some automorphism φ of L. Hence, $\vec{h}' = \vec{h}$ in this case since otherwise (6.16) (with notational changes and equality instead of inequality in the middle) would lead to a contradiction. We have shown (6.21).

Next, continuing the argument for Fact 6.8, assume that $\vec{h} \in \Gamma$. By (6.14) and (6.15), $\text{typ}(\vec{h}) \notin \{(4,0), (0,4), (2,2)\}$. Hence, $\text{typ}(\vec{h}) = (3,1) = \text{typ}(\vec{g})$ or $\text{typ}(\vec{h}) = (1,3) = \text{typ}(\vec{g}')$. Since L is selfdual by Fact 6.2 (or since the second alternative needs almost the same treatment), we can assume that $\text{typ}(\vec{h}) = (3,1) = \text{typ}(\vec{g})$. Then $\vec{h} \in \Gamma$ and $\vec{g} \in \Gamma$ have the same role. Hence (6.20) applies to $\vec{h}$ and $\vec{g}'$, whence $\text{ftyp}(\vec{h})$ and $\text{ftyp}(\vec{g}')$ are complementary. As only one fine type is complementary to $\text{ftyp}(\vec{g}')$, we have that $\text{ftyp}(\vec{h}) = \text{ftyp}(\vec{g})$. Thus, (6.21) yields that $\vec{h} = \vec{g}$. So $\vec{h} = \vec{g} \in \{\vec{g}, \vec{g}'\}$, implying that $k = 2$ and completing the proof of Fact 6.8.

Next, assume that $k > 2$. We know from (6.14) and (6.15) that, for all $i \in [k]$, $\text{typ}(\vec{g}^{(k)}) \notin \{(4,0), (2,2), (0,4)\}$. So $\text{typ}(\vec{g}^{(1)}) \in \{(3,1), (1,3\}$. By duality, we can assume that $\text{typ}(\vec{g}^{(1)}) = (3,1)$. As Fact 6.8 together with $k > 2$ exclude that $\text{typ}(\vec{g}^{(i)}) = (1,3)$ for some $i \in [k] \setminus \{1\}$, we have that $\text{typ}(\vec{g}^{(i)}) = (3,1)$ for all $i \in [k]$. Hence, for every $i \in [k]$, $\text{ftyp}(\vec{g}^{(i)})$ is one of the fine types $(1,1,1,2)$, $(1,1,2,1)$, $(1,2,1,1)$, and $(2,1,1,1)$. Since each of these four fine types occurs at most once by (6.21), it follows that $k \leq 4$, proving (6.8).

Clearly, (6.8), the first inequality in (3.4), and the particular $(t,d) = (0,3)$ case of (the already proven) (3.8) and (6.8) imply (3.10).

Next, interrupting the proof of Theorem 3.2, we recall and, for the reader's convenience, prove the following lemma; its first part follows from known deep results.

Lemma 6.9 (Day and Pickering [5], Herrmann [10], Hermmann and Huhn [11])**.** *Every complete quadrangle $\vec{p} = (p_1, p_2, p_3, p_4)$ in P_2 (the projective plane over the* prime *field F) is a generating vector of $L = \text{Sub}(P_2)$. So is every quadruple $\vec{q}$ in general position such that* $\text{typ}(\vec{q}) \neq (2,2)$.

In the context of this paper, the proof of Lemma 6.9 is straightforward and, what is important in Section 8, it does not rely on Gelfand and Ponomarev's result, which was mentioned after (2.3). Here, we provide a concise demonstration. (6.12) shows that the assumption $\mathrm{typ}(\vec{q}) \neq (2,2)$ cannot be omitted from the lemma.

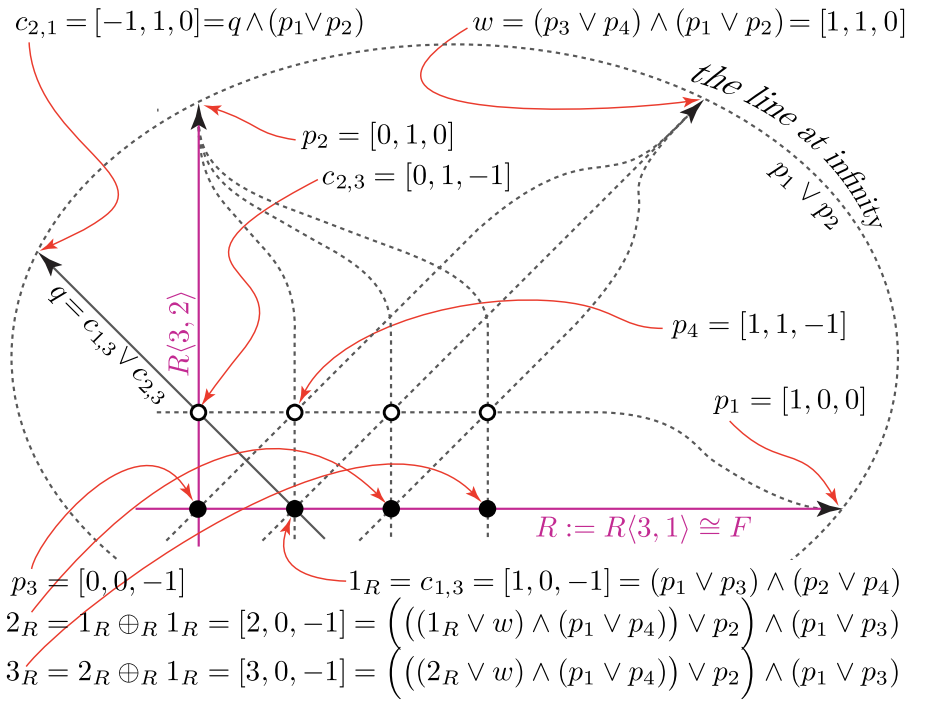

FIGURE 9. Generating the (subspace lattice of the) projective plane

Proof of Lemma 6.9. Let $\vec{p}$ be a complete quadrangle. By Fact (6.5), we can assume that $\vec{p}$ is the canonical complete quadrangle; see Figure 9. Let $S := [p_i : i \in [4]]_{\mathrm{lat}}$. The figure shows that the elements of the canonical von Neumann 3-frame, $a_i := p_i$ for $i \in [3]$ and $c_{i,j} = c_{j,i}$ for $i \neq j \in [3]$, are in S. In particular, $1_{R\langle 3,1\rangle} = c_{1,3} \in S$. As $R\langle 3,1\rangle \cong F$ by Theorem 4.1, $R\langle 3,1\rangle$ is a prime field and so it is generated by $1_{R\langle 3,1\rangle}$. Therefore, since S is closed with respect to the field operations by (4.11), $R\langle 3,1\rangle \subseteq S$. In virtue of (5.21), we can apply (5.20) to conclude that $S = L$, as required. This proves the first half of Lemma 6.9.

To show the second half, (6.12), the first half of Lemma 6.9, and duality allow us to assume that $\mathrm{typ}(\vec{q}) = (3,1)$. We can assume that q_1, q_2, q_3 are points and q_4 is a line. Letting $\vec{q}$ play the role of $\vec{g}$ on the left of Figure 8, we obtain that $\{a_{24}, a_{34}\} \subseteq [q_1, \ldots, q_4]_{\mathrm{lat}} =: S$. So S contains a complete quadrangle, $(q_2, q_3, a_{24}, a_{34})$, whereby the first part of the lemma implies that $S = L$, as required. We have proved Lemma 6.9. □

To complete the proof of Theorem 3.2, we need to show (3.9). With its assumptions, if $f^{\mathrm{mng}}(L^k) \leq 3$, then Remark 3.4 would give that $f^{\mathrm{mng}}(L) \leq 3$, contradicting (3.4). Hence, $f^{\mathrm{mng}}(L^k) \geq 4$. By Remark 3.4, it suffices to prove

that L^4 has a 4-element generating set. Let e be a line and a, b, c be three non-collinear points of the projective plane such that none of these points lies on e. Then the quadruple (e, a, b, c) is in general position; think of the left of Figure 8 and $(e, a, b, c, e) := (g_4, g_1, g_2, g_3)$.) Keeping the explanatory sentence right after Lemma 6.1 in mind, take the matrix

$$U = (u_{i,j})_{4\times 4} := \begin{pmatrix} e & a & b & c \\ a & e & b & c \\ a & b & e & c \\ a & b & c & e \end{pmatrix},$$

and let $\vec{g}^{(i)} = (u_{i,1}, u_{i,2}, u_{i,3}, u_{i,4})$ be the i-th row of U for $i \in [4]$. With $\vec{\xi} = (\xi_1, \xi_2, \xi_3, \xi_4)$ as a vector of variables, define the following quaternary lattice terms for $i, j \in [4]$, $i \neq j$:

$$\begin{aligned} w_i(\vec{\xi}) &:= \bigwedge_{j\in[4]\setminus\{i\}} (\xi_i \vee \xi_j), \\ h_{i,j}(\vec{\xi}) &:= \xi_j \wedge \bigwedge_{s\in[4]\setminus\{i,j\}} \bigl(w_i(\vec{\xi}) \vee \xi_s\bigr), \text{ and} \\ f_i^{(\mathrm{e})}(\vec{\xi}) &:= \bigvee_{j\in[4]\setminus\{i\}} h_{i,j}(\vec{\xi}). \end{aligned} \tag{6.22}$$

The superscript (e) of f_i will be a useful reminder later. Some substitution values of these terms are given as follows:

ξ_1	ξ_2	ξ_3	ξ_4	$w_1(\vec{\xi})$	$h_{1,2}(\vec{\xi})$	$h_{1,3}(\vec{\xi})$	$h_{1,4}(\vec{\xi})$	$f_1^{(\mathrm{e})}(\vec{\xi})$
e	a	b	c	1	a	b	c	1
a	e	b	c	a	0	0	0	0
a	b	e	c	a	0	0	0	0
a	b	c	e	a	0	0	0	0

The last column above shows that $f_1^{(\mathrm{e})}(\vec{g}^{(j)}) = \delta_{1j}^{(L)}$. By symmetry or by three additional similar tables,

$$f_i^{(\mathrm{e})}(\vec{g}^{(j)}) = \delta_{ij}^{(L)} \text{ holds for all } i, j \in [4]. \tag{6.23}$$

Note for later reference that all we needed to prove (6.23) is only that

$$\mathrm{ftyp}(a, b, c, e) = (1, 1, 1, 2) \text{ and } (a, b, c, e) \text{ is in general position.} \tag{6.24}$$

By (6.23), Condition (2) of Lemma 6.1 holds. So does Condition (1) of the same lemma by the second half of Lemma 6.9. Thus, the columns of U form a 4-element generating set of L^4 by Lemma 6.1, completing the proof of (3.9) and that of Theorem 3.2. □

7. Proving Theorem 3.3 and Example 3.6

Proof of Theorem 3.3. If λ is infinite, then $|L| = 2^{\aleph_0}$ and so L is not finitely generated. (In fact, it is not even $\aleph_0$-generated.) If a prime field F occurred at least five times in the direct product (3.11) and L was 4-generated, then $\mathrm{Sub}({}_F F^3)^5$ would also be 4-generated by Remark 3.4, contradicting (3.10). Thus, the condition right after (3.11) is necessary. The rest of the proof assumes this condition. We need to prove that $f^{\mathrm{mng}}(L) = 4$. In fact, it suffices to find an at most 4-element generating set since the assumption $\lambda \neq 0$ together with (3.4) and Remark 3.4 imply that

$f^{\mathrm{mng}}(L) \geq 4$. Furthermore, by Remark 3.4 again, we can assume that each prime field occurs exactly four times. So, taking (4.1) also into account, we assume that

$$L = \prod_{i\in[k]} \prod_{\nu\in[4]} L_{i,\nu}, \text{ where } L_{i,\nu} = \mathrm{Sub}(P_2(F_i)), \quad F_i \ncong F_j$$

for $i \neq j$, and we construct an (at most) 4-element generating set of L.

For $i \in [k]$, let p_1^i, p_2^i, p_3^i, and p_4^i be the points (and also the atoms in the corresponding subspace lattice) $[1,0,0]$, $[0,1,0]$, $[0,0,-1]$, and $[1,1,-1]$ in the projective plane $P_2^i := P_2(F_i)$ over F_i, respectively; see Figure 9 where the superscript i is never indicated. Let $c_{2,3}^i := (p_1^i \vee p_4^i) \wedge (p_2^i \vee p_3^i)$. Figure 9 shows how we define $c_{1,3}^i$, $c_{2,1}^i$, and (for later use) w^i. We let

$$q^i := c_{1,3}^i \vee c_{2,3}^i \text{ and } \vec{r}^{(i)} := (p_1^i, p_2^i, p_3^i, q^i).$$

Figure 9 shows and it is easy to verify that

$$p_4^i = \Big(\big((p_1^i \vee p_3^i) \wedge q^i\big) \vee p_2^i\Big) \wedge \Big(\big((p_2^i \vee p_3^i) \wedge q^i\big) \vee p_1^i\Big). \tag{7.1}$$

For $i \in [k]$, we define the following four quadruples:

$$\vec{r}^{(i,1)} := (q^i, p_1^i, p_2^i, p_3^i), \qquad \vec{r}^{(i,2)} := (p_1^i, q^i, p_2^i, p_3^i) \tag{7.2}$$

$$\vec{r}^{(i,3)} := (p_1^i, p_2^i, q^i, p_3^i), \qquad \vec{r}^{(i,4)} := (p_1^i, p_2^i, p_3^i, q^i) = \vec{r}^{(i)}. \tag{7.3}$$

Form a $([k]\times[4])$-by-4 matrix from these vectors as row vectors. So the rows of this matrix are indexed by pairs taken from $[k]\times[4]$ and there are four columns. The (i,ν)-th row of the matrix is $\vec{r}^{(i,\nu)}$. We claim that the four columns of the matrix generate L. To prove this, we need to verify both conditions given in Lemma 6.1. The satisfaction of Condition (1) of Lemma 6.1 follows from the second half of Lemma 6.9; it also follows from (7.1) and the first half of Lemma 6.9.

Let $\vec{\xi}$ stand for the vector $(\xi_1, \xi_2, \xi_3, \xi_4)$ of variables. To show that Condition (2) of Lemma 6.9 also holds and to complete the proof of the theorem, it suffices to define quaternary lattice terms $f_{i,\nu} = f_{i,\nu}(\vec{\xi})$ for $(i,\nu) \in [k]\times[4]$ such that for any $(j,\kappa) \in [k]\times[4]$,

$$f_{i,\nu}(\vec{r}^{(j,\kappa)}) = \begin{cases} 1_{L_j}, & \text{if } (j,\kappa) = (i,\nu), \\ 0_{L_j}, & \text{if } (j,\kappa) \neq (i,\nu). \end{cases} \tag{7.4}$$

The term $f_{i,\nu}$ that we define is of the form

$$f_{i,\nu}(\vec{\xi}) := g_{i,\nu}(\vec{\xi}) \wedge f_\nu^{(\mathrm{e})}(\vec{\xi}), \text{ where } f_\nu^{(\mathrm{e})} \text{ is taken from (6.22).} \tag{7.5}$$

(The superscript "(e)" in (7.5) comes from "earlier".) Note that almost all of the terms we define in the rest of the proof are quaternary terms on $\vec{\xi}$ but $\vec{\xi}$ will often be dropped. As the components in (7.2)–(7.3) are permuted cyclically, we do the same with the variables of $g_{i,\nu}$. So we define, in several steps, $g_{i,4}$; then, in harmony with (7.2)–(7.3), the rest of the terms $g_{i,\nu}$ are given by the following rules:

$$g_{i,1}(\vec{\xi}) := g_{i,4}(\xi_4, \xi_1, \xi_2, \xi_3), \tag{7.6}$$

$$g_{i,2}(\vec{\xi}) := g_{i,4}(\xi_1, \xi_4, \xi_2, \xi_3), \text{ and} \tag{7.7}$$

$$g_{i,3}(\vec{\xi}) := g_{i,4}(\xi_1, \xi_2, \xi_4, \xi_3), \tag{7.8}$$

Keeping an eye on Figure 9, $R = R^i =: R\langle 3,1\rangle$ will also stand for F_i. In the figure, $0_R^i := 0_{R^i}$, $1_R^i = c_{1,3}$, $2_R^i = [2,0,-1]$, and $3_R^i = [3,0,-1]$ are already given.

(As we have already mentioned, i is not indicated in the figure.) For all $s \in \mathbb{N}^+$, we defined $s^i_R \in L_i$ by induction as follows:

$$(s+1)^i_R := s^i_R \oplus_R 1^i_R = \Big(\big((s^i_R \vee w^i) \wedge (p^i_1 \vee p^i_4)\big) \vee p^i_2\Big) \wedge (p^i_1 \vee p^i_3). \tag{7.9}$$

$$\text{Clearly, for all } s \in \mathbb{N}^+, \text{ we have that } s^i_R = [s, 0, -1] \in L_i; \tag{7.10}$$

this follows also from Theorem 4.1. When defining lattice terms for a given $i \in [k]$, c^{*i} and c^{**i} denote terms closely related to a point $c \in P^i_2$; we usually drop i if such a term does not depend on it. First, to get rid of p^i_4 and bring q^i in, we replace p^i_4 with the right-hand side of (7.1) in every expression in Figure 9. In harmony with (7.1), (7.9), and Figure 9, we let

$$p^*_4 = p^*_4(\vec{\xi}) := \Big(\big((\xi_1 \vee \xi_3) \wedge \xi_4\big) \vee \xi_2\Big) \wedge \Big(\big((\xi_2 \vee \xi_3) \wedge \xi_4\big) \vee \xi_1\Big),$$

$$w^* = w^*(\vec{\xi}) := (\xi_3 \vee p^*_4) \wedge (\xi_1 \vee \xi_2), \quad p^*_\nu = p^*_\nu(\vec{\xi}) := \xi_\nu \text{ for } \nu \in [3], \tag{7.11}$$

$$0^* = 0^*(\vec{\xi}) := \xi_3, \text{ and for } s \in \mathbb{N}_0, \tag{7.12}$$

$$(s+1)^* = (s+1)^*(\vec{\xi})$$

$$:= \Big(\big((s^* \vee w^*) \wedge (\xi_1 \vee p^*_4)\big) \vee \xi_2\Big) \wedge (\xi_1 \vee \xi_3). \tag{7.13}$$

$$\text{Let } c^*_{1,3} = c^*_{1,3}(\vec{\xi}) := 1^* \text{ and } c^*_{2,3} = c^*_{2,3}(\vec{\xi}) := 1^*(\xi_2, \xi_1, \xi_3, \xi_4). \tag{7.14}$$

So $0^*, 1^*, 2^*, \dots$ are lattice terms, not numbers. Comparing (7.9), (7.10), (7.12), and (7.13), we obtain that for all $j \in [k]$ and $s \in \mathbb{N}_0$,

$$s^*(\vec{r}^{(j)}) = [r, 0, -1] =: r^j_R \in L_j. \tag{7.15}$$

By construction and since the subscripts 1 and 2 share a symmetrical role, for any $j \in [k]$ and $\iota \in [4]$,

$$p^*_\iota(\vec{r}^{(j)}) = p^j_\iota, \ w^*(\vec{r}^{(j)}) = w^j, \ c^*_{1,3}(\vec{r}^{(j)}) = c^j_{1,3}, \ c^*_{2,3}(\vec{r}^{(j)}) = c^j_{2,3}. \tag{7.16}$$

To define further terms, we need to distinguish between two cases.

First, assume that $t_i := |F_i|$ is a prime number. We let

$$p^{**i}_3 = p^{**i}_3(\vec{\xi}) := p^*_3 \wedge (t_i)^*, \tag{7.17}$$

$$p^{**i}_1 = p^{**i}_1(\vec{\xi}) := p^{*i}_1 \wedge (p^{**i}_3 \vee p^{*i}_2 \vee p^{*i}_4),$$

$$p^{**i}_2 = p^{**i}_2(\vec{\xi}) := p^{*i}_2 \wedge (p^{**i}_3 \vee p^{*i}_1 \vee p^{*i}_4), \text{ and}$$

$$p^{**i}_4 = p^{**i}_4(\vec{\xi}) := p^{*i}_4 \wedge (p^{**i}_3 \vee p^{*i}_1 \vee p^{*i}_2).$$

We claim that for all $\iota \in [4]$ and $j \in [k]$,

$$\text{in the lattice } L_j, \quad p^{**i}_\iota(\vec{r}^{(j)}) = \begin{cases} p^j_\iota, & \text{if } j = i, \\ 0_{L_j} & \text{if } j \neq i. \end{cases} \tag{7.18}$$

To show this, observe that we know from (7.15) and (7.16) that both $p^*_3(\vec{r}^{(j)}) = 0^j_R$ and $(t_i)^*(\vec{r}^{(j)}) = (t_i)^j_R$ are points on the solid (magenta) horizontal line $p^j_3 \vee p^j_1$ in Figure 9. If $j \neq i$, then $F_j \not\cong F_i$, $0^j_R \neq (t_i)^j_R$, and the meet of these two distinct points is $p^{**i}_3(\vec{r}^{(j)}) = \emptyset = 0_{L_j}$. If $j = i$, then 0^j_R and $(t_i)^j_R$ are equal, whereby their meet is $p^{**i}_3(\vec{r}^{(j)}) = 0^j_R = p^j_3$. This shows the validity of (7.18) for $\iota = 3$. Based on (7.16) and Figure 9, we conclude (7.18) from its particular case $\iota = 3$.

Second, we assume that $F_i = \mathbb{Q}$, the field of rational numbers. Everything goes in the very same way as in the previous case when F_i was finite except that (7.17) and the corresponding argument for the $\iota = 3$ case of (7.18) need some modifications. As a preparation to this task, with self-explanatory substitutions and using the terms (7.11)–(7.14), we turn (5.3) with $(i, j, k) = (3, 1, 2)$ into the quinary lattice term

$$\mathrm{rec}^*_{312}(x, \vec{\xi}) := \Big(\Big(\Big(\big((x \vee c^*_{2,3}) \wedge (p^*_1 \vee p^*_2)\big) \vee c^*_{1,3}\Big)\Big) \\ \wedge (p^*_2 \vee p^*_3) \vee c^*_{2,1}\Big) \wedge (p^*_3 \vee p^*_1).$$

With $T := \{|F_j| : j \in [k] \text{ and } F_j \text{ is finite}\}$, let

$$p_3^{**i} = p_3^{**i}(\vec{\xi}) := p^*_3 \wedge \bigwedge_{t \in T} \Big(p^*_1 \vee \mathrm{rec}^*_{312}(t^*(\vec{\xi}))\Big). \tag{7.19}$$

We claim that (7.18) for $\iota = 3$ still holds. If $i = j$, then $F_j \cong \mathbb{Q}$ and for every $t \in T$, $t^*(\vec{r}^{(j)}) = t^j_R$ is not the zero element of $R^j \cong \mathbb{Q}$ by (7.15). Hence, Lemma 5.2 implies that $\mathrm{rec}^*_{312}(t^*(\vec{r}^{(j)})) = \mathrm{rec}^*_{312}(t^j_R) = (1/t)^j_R$ belongs to R^j. In particular, $(1/t)^j_R$ is distinct from p^j_1, the infinite point of the (solid magenta) horizontal axis. This fact and the first equality in (7.16) yield that the join in (7.19) turns into $p^j_1 \vee (1/t)^j_R$, which is the (magenta) solid horizontal line in Figure 9. As this line contains $p^*_3(\vec{r}^{(j)}) = p^j_3$, we have that $p_3^{**i}(\vec{r}^{(j)}) = p^j_3$ for $j = i$, as required.

Now let us examine what happens if $j \neq i$. Then the prime number $t := |F_j|$ is in T and the join $p^*_1 \vee \mathrm{rec}^*_{312}(t^*(\vec{\xi}))$ is one of the meetands in (7.19). By (7.16), $t^*(\vec{r}^{(j)}) = t^j_R = 0^j_R = p^j_3$. We know from Lemma 5.2 that $\mathrm{rec}_{312}(p^j_3)$ is p^j_1. Thus, using (7.16) again, the meetand $p^*_1 \vee \mathrm{rec}^*_{312}(t^*(\vec{\xi}))$ turns into $p^j_1 \vee p^j_1 = p^j_1$ when $\vec{r}^{(j)}$ is substituted for $\vec{\xi}$. Since p^*_3 turns into p^j_3 after the substitution and $p^j_3 \wedge p^j_1 = 0_{L_j}$, we have that $p_3^{**i}(\vec{r}^{(j)}) = 0_{L_j}$, as required. We have shown that (7.18) for $\iota = 3$ still holds. Based on (7.16), we conclude (7.18) from its particular case $\iota = 3$.

We have seen that not matter if F_i is finite or not, (7.18) holds for all $i, j \in [k]$ and $\iota \in [4]$. This allows us to let

$$g_{i,4}(\vec{\xi}) := \bigvee_{\iota \in [4]} p_\iota^{**i}(\vec{\xi}); \tag{7.20}$$

then (7.6), (7.7), and (7.8) define $g_{i,\nu}(\vec{\xi})$ for $\nu \in [3]$.

Since the "rotational symmetry" of (7.2)–(7.3) and that of (7.6), (7.7), and (7.8) correspond to each other, it suffices to verify (7.4) only for $\nu = 4$. So we are examining $f_{i,4}(\vec{r}^{(j,\kappa)}) = g_{i,4}(\vec{r}^{(j,\kappa)}) \wedge f^{(\mathrm{e})}_4(\vec{r}^{(j,\kappa)})$; see (7.5).

First, assume that $(j, \kappa) = (i, 4)$. Then the definition of $f^{(\mathrm{e})}_4$ in (6.22) does not depend on the underlying field and neither the argument showing (6.23) does, whence it follows from (6.23) and (6.24) that $f^{(\mathrm{e})}_4(\vec{r}^{(j,\kappa)}) = f^{(\mathrm{e})}_4(\vec{r}^{(i)}) = 1_{L_i} = 1_{L_j}$. All the joinands in (7.20) are the respective points by (7.18). As these points are in general position, we have that $g_{i,4}(\vec{r}^{(j,\kappa)}) = 1_{L_j}$. Thus, $f_{i,4}(\vec{r}^{(j,\kappa)}) = 1_{L_j}$, as (7.4) requires. Next, assume that $(j, \kappa) \neq (i, 4)$. If $\kappa \neq 4$, then (6.23) and (6.24) give that $f^{(\mathrm{e})}_4(\vec{r}^{(j,\kappa)}) = 0_{L_j}$, implying that $f_{i,4}(\vec{r}^{(j,\kappa)}) = 0_{L_j}$, as required. If $j \neq i$, then (7.18) implies that all the joinands in (7.20) turn into 0_{L_j} when $\vec{r}^{(j,\kappa)}$ is substituted for $\vec{\xi}$, whereby $g_{i,4}(\vec{r}^{(j,\kappa)}) = 0_{L_j}$ and so $f_{i,4}(\vec{r}^{(j,\kappa)}) = 0_{L_j}$ again, as required. Now that we have proved (7.4), the proof of Theorem 3.3 is complete. □

Proof of Remark 3.7. It suffices to exclude that $F = \mathbb{Q}(u)$ for some $u \in F$. Suppose the contrary and pick such a u. Then u is transcendental and $\sqrt[80]{80} = f(u)/g(u)$ for some polynomials $f \in \mathbb{Q}[x]$ and $g \in \mathbb{Q}[x] \setminus \{0\}$. Since u is a root of the polynomial $f(x)^{80} - 80g(x)^{80} \in \mathbb{Q}[x]$, this polynomial is 0. Hence, with a $q \in \mathbb{Q}$ such that $g(q) \neq 0$, $80 = (f(q)/g(q))^{80}$. Thus $\sqrt[80]{80} = f(q)/g(q) \in \mathbb{Q}$, which is a contradiction, as required. □

Proof of Example 3.6. By the well-known multiplicativity of degrees and the primitive element theorem, see for example Milne [13, Proposition 1.20 and Theorem 5.1], F in Part (a) is $t = 1$-generated. Hence, Part (a) follows from (3.4) and (3.8). As the elements β_i are independent, $t := f^{\mathrm{mng}}(F)$ in Part (b) equals 80 by the fundamental theorem on transcendence bases; see for example Theorem 9.5 in Milne [13]. Therefore, (3.4) and (3.7) imply Part (b). (3.4) and (3.8) imply Part (c). To verify Part (d) for $|F| = 19$, note that $k = 10^{2046}$ is smaller than μ in (3.6) by Table 1. If $F = \mathbb{Q}$, then $k \leq \mu = \aleph_0$ is trivial. Hence, L^k is 5-generated by (3.8). Since $f^{\mathrm{mng}}(\mathbb{A}) = \aleph_0$, (3.7) implies Part (e). Finally, even without Remark 3.7, Part (f) follows from (3.4) and (3.8) since $t = f^{\mathrm{mng}}(F) \in \{1, 2\}$. □

8. Appendix: Extracting Gelfand and Ponomarev's result from Zádori's proof

A lot in this paper depends on Gelfand and Ponomarev's theorem:

Theorem 8.1 (Gelfand and Ponomarev [7])**.** *If $3 \leq n \in \mathbb{N}^+$, K is a prime field, and $V = K^n$ is the n-dimensional vector space over K, then the subspace lattice $L(K^n) := \mathrm{Sub}(V)$ has a 4-element generating set.*

At the time of writing, the *old* website http://www.acta.hu/ of Acta Sci. Math. (Szeged) provides free access to Zádori's paper [22], while Gelfand and Ponomarev's proof seems to be less available. Thus, we recall Zádori's construction briefly and point out how it proves Theorem 8.1.

Given a prime field K, an expression like $[-x, x, 0, 0, -2y, z, x + y]_{\mathrm{vs}}$ stands for the subspace $\{(-x, x, 0, 0, -2y, z, x + y) \in K^7 : x, y, z \in K\}$. The subscript "vs" (from "vector space") distinguishes this subspace from the projective point $[-x, x, 0, 0, -2y, z, x + y]$ in the projective space $P_6(K)$. Letting $c := 1$ in his paper [22], Zádori's five subspaces turn into the following four subspaces.

Definition 8.2 (Zádori's subspaces [22, for $c = 1$])**.** For $n = 2k + 1 \geq 3$, let

$$\begin{aligned} t_1 = t_1^{(n)} &:= [0, \ldots, 0, x_{k+1}, \ldots, x_{2k+1}]_{\mathrm{vs}}, \\ t_2 = t_2^{(n)} &:= [x_1, \ldots, x_k, 0, \ldots, 0]_{\mathrm{vs}}, \\ t_3 = t_3^{(n)} &:= [x_1, \ldots, x_k, 0, x_1, \ldots, x_k]_{\mathrm{vs}}, \text{ and} \\ t_4 = t_4^{(n)} = t_5 = t_5^{(n)} &:= [x_1, \ldots, x_k, x_1, \ldots, x_k, 0]_{\mathrm{vs}}. \end{aligned}$$

Furthermore, for $n = 2k \geq 4$, let

$$\begin{aligned} t_1 = t_1^{(n)} &:= [0, \ldots, 0, x_{k+1}, \ldots, x_{2k}]_{\mathrm{vs}}, \\ t_2 = t_2^{(n)} &:= [x_1, \ldots, x_k, 0, \ldots, 0]_{\mathrm{vs}}, \\ t_3 = t_3^{(n)} &:= [x_1, \ldots, x_k, x_1, \ldots, x_k]_{\mathrm{vs}}, , \text{ and} \\ t_4 = t_4^{(n)} = t_5 = t_5^{(n)} &:= [0, x_2, \ldots, x_k, x_2, \ldots, x_k, 0]_{\mathrm{vs}}. \end{aligned}$$

Proof Theorem 8.1, which is the particular $c = 1$ case of Zádori [22]. Let $T^{(n)} := \{t_1^{(n)}, \ldots, t_4^{(n)}\}$, and let $[T^{(n)}]_{\mathrm{lat}}$ stand for the sublattice of $L(K^n)$ generated by $T^{(n)}$. It suffices to show that $[T^{(n)}]_{\mathrm{lat}} = L(K^n)$. For $n = 3$, $\{t_1^{(n)}, \ldots, t_4^{(n)}\}$ generates $L := \mathrm{Sub}({}_K K^n) \cong \mathrm{Sub}(P_2(K))$ by Lemma 6.9 and Figure 9. The same holds for all $3 \leq n \in \mathbb{N}^+$, because the induction step from $\{n-2, n-1\}$ to n is the same as in Zádori [22], provided that we keep $c = 1$ and let $t_8 := t_7$ and $t_{12} := t_{11}$ there. This is how Zádori [22] proves Theorem 8.1.

The proof is ready at this point. However, for the reader's convenience and also because we can benefit from Section 4, we give more details. Note that although (8.1) is not in Zádori's paper, this does not mean a significant difference from his argument.

In what follows, using the case $n = 3$ as the base of induction, we present the induction step. Actually, we present two sorts of induction steps; one for n even and one for n odd. But first, we formulate and prove an auxiliary statement; see (8.1) a bit later. For $u \in L(K^n)$, $\mathrm{idl}(u)$ will denote the *principal ideal* $\{v \in L(K^n) : v \leq u\}$. We claim that if we consider the following hyperplane

$$H_i := [x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n]_{\mathrm{vs}}$$

and G is a subspace of K^n such that $G \not\subseteq H_i$ and $\dim G \geq 2$, then

$$\mathrm{idl}(G) \cup \mathrm{idl}(H_i) \text{ generates } L(K^n). \tag{8.1}$$

It suffices to prove (8.1) only in the case when $i = n$ and $\dim G = 2$. In this case, after passing from V to the projective space P_{n-1} over K, G is a line of P_{n-1} and H_n is a hyperplane with codimension 1, that is, H_n is a coatom in $\mathrm{Sub}(P_{n-1})$. We treat H_n as the hyperplane at infinity. Let S stand for the sublattice generated by $\mathrm{idl}(G) \cup \mathrm{idl}(H_n)$ in $\mathrm{Sub}(P_{n-1})$. Let $p \in P_{n-1}$ be an arbitrary point, that is, $\{p\}$ (which we denote by p according to the conventions of the paper) is an atom of $\mathrm{Sub}(P_{n-1})$. We are going to show that $p \in S$. We can assume that $p \notin \mathrm{idl}(G) \cup \mathrm{idl}(H_n)$ in $\mathrm{Sub}(P_{n-1})$, as otherwise $p \in S$ is obvious. In particular, $p \notin H_n$ (understood geometrically), that is, p is a finite point. We know (say, from Grätzer [8, page 376]) that whenever a subspace contains two distinct points of a line, then it contains all points of the line in question. We also know that each line has at least three points. Hence, it follows from $G \not\subseteq H_n$ and (4.1) that $G \setminus H_n$ contains two distinct points, q_1 and q_2. Since $p \notin G = \ell_{q_1,q_2}$, we have that $\ell_{p,q_1} \neq \ell_{p,q_2}$, and so $p = \ell_{p,q_1} \wedge \ell_{p,q_2}$ in $\mathrm{Sub}(P_{n-1})$. For $i \in [2]$, let r_i denote the point at infinity on the line ℓ_{p,q_i}; r_i exists since each line has at least one point at infinity, it is in the hyperplane H_n, and it is uniquely determined since the finite points p, q_i on ℓ_{p,q_i} exclude that $\ell_{p,q_i} \subseteq H_n$. As p, q_i, and r_i are three distinct points on the same line, we have that

$$p = \ell_{p,q_1} \wedge \ell_{p,q_2} = \ell_{r_1,q_1} \wedge \ell_{r_2,q_2} = (r_1 \vee q_1) \wedge (r_2 \vee q_2) \in S,$$

proving the validity of (8.1).

Next, to perform the induction step from $n-1$ (and, for an odd n, also from $n-2$) to n, first we deal with the case when $4 \leq n = 2k$ is even. Then we define[12]

$$t_6^{(n)} := (t_1^{(n)} \vee t_4^{(n)}) \wedge t_2^{(n)} = [0, x_2, \ldots, x_k, 0, \ldots, 0]_{\mathrm{vs}} \text{ and}$$
$$t_7^{(n)} := (t_1^{(n)} \vee t_4^{(n)}) \wedge t_3^{(n)} = [0, x_2, \ldots, x_k, 0, x_2, \ldots, x_k]_{\mathrm{vs}}.$$

Let $B := \{t_1^{(n)}, t_6^{(n)}, t_7^{(n)}, t_4^{(n)}\}$; it is a subset of $[T^{(n)}]_{\mathrm{lat}}$. Since B is the image of $T^{(n-1)}$ under the "natural[13] isomorphism" $K^{n-1} \to [0, x_2, \ldots, x_n]_{\mathrm{vs}} = H_1$, the induction hypothesis implies that $G := \mathrm{idl}(H_1) \subseteq [T^{(n)}]_{\mathrm{lat}}$. Since $T^{(n)}$ is invariant under the automorphism $K^n \to K^n$ defined by $(x_1, \ldots, x_n) \mapsto (x_n, \ldots, x_1)$, $\mathrm{idl}(H_n) \subseteq [T^{(n)}]_{\mathrm{lat}}$ also holds. Hence, (8.1) implies that $[T^{(n)}]_{\mathrm{lat}} = L(K^n)$, as required.

Second, we assume that $n = 2k+1 \geq 5$. Then $[T^{(n)}]_{\mathrm{lat}}$ contains

$$t_6^{(n)} := (t_2^{(n)} \vee t_3^{(n)}) \wedge t_1^{(n)} = [0, \ldots, 0, x_{k+2}, \ldots, x_{2k+1}]_{\mathrm{vs}},$$
$$t_7^{(n)} := (t_2^{(n)} \vee t_3^{(n)}) \wedge t_4^{(n)} = [0, x_2, \ldots, x_k, 0, x_2, \ldots, x_k, 0]_{\mathrm{vs}}$$
$$t_9^{(n)} := (t_2^{(n)} \vee t_4^{(n)}) \wedge t_1^{(n)} = [0, \ldots, 0, x_{k+1} \ldots, x_{2k}, 0]_{\mathrm{vs}}$$
$$t_{10}^{(n)} := (t_2^{(n)} \vee t_4^{(n)}) \wedge t_3^{(n)} = [x_1, \ldots, x_{k-1}, 0, 0, x_1, \ldots, x_{k-1}, 0]_{\mathrm{vs}}$$
$$t_{11}^{(n)} := (t_9^{(n)} \vee t_{10}^{(n)}) \wedge t_4^{(n)} = [x_1, \ldots, x_{k-1}, 0, x_1, \ldots, x_{k-1}, 0, 0]_{\mathrm{vs}}$$
$$t_{13}^{(n)} := (t_9^{(n)} \vee t_{10}^{(n)}) \wedge t_2^{(n)} = [x_1, \ldots, x_{k-1}, 0, \ldots, 0]_{\mathrm{vs}}$$

Since $\{t_6^{(n)}, t_2^{(n)}, t_3^{(n)}, t_7^{(n)}\}$ corresponds to $T^{(n-1)}$ under the "natural isomorphism" $K^{n-1} \to H_{k+1}$, the induction hypothesis gives that $\mathrm{idl}(H_{k+1}) \subseteq [T^{(n)}]_{\mathrm{lat}}$. As $\{t_9^{(n)}, t_{13}^{(n)}, t_{10}^{(n)}, t_{11}^{(n)}\}$ corresponds to $T^{(n-2)}$ under the "natural isomorphism" $K^{n-2} \to H_k \cap H_n := G$, the induction hypothesis yields also that $\mathrm{idl}(G) \subseteq [T^{(n)}]_{\mathrm{lat}}$. Since $G \not\subseteq H_{k+1}$ and $\dim(G) = n-2 \geq 3 \geq 2$, we can use (8.1) (with $i := k+1$) to conclude that $[T^{(n)}]_{\mathrm{lat}} = L(K^n)$, completing the induction step and the proof of Theorem 8.1. □

9. Appendix: the Maple program mentioned in Footnote 11

This section presents two Maple programs.

The following short program computed the data Table 1.

```
> restart; #with(combinat):
> gbc:=proc(q,m,r) local i,j,k,sz,nev,thisisit;
>   sz:=1; nev:=1;
>  for i from m-r+1 to m do  sz:=sz*(1-q^i) od;
>  for i from 1 to r do nev:=nev*(1-q^i) od;
>  thisisit:=round(evalf(sz/nev));
> end:
> for q from 2 to 19 do
>  if member(q, {2,3,4,5,7,8,9,11,13,16,17,19})
```

[12]There will be no t_5 in this paper and there will be other gaps in the set of subscripts later. This makes it easier to see that the subspaces defined here are exactly the "$c := 1$ cases of the subspaces" given in Zádori [22], but now we do not need all of his subspaces.

[13]We use quotation marks around "natural" to indicate that not in a category theoretic sense.

```
>  then d:=80: ehat:=gbc(q,d,floor(d/2)): print(" "):
>   print(cat("d=",d,", q=",q," d chooses d/2 w.r.t. q=",
>    ehat,", and its log[10]=", evalf(log[10](ehat)) )):
>  fi:
> od:
```

We continue with the Maple program mentioned in Footnote 11.

```
> restart; #Computation in the Fano plane
> # The program contains some parts, called "tests". Running
> # these parts can increase your trust in the program.
> # To run these parts, delete the hash marks (#) from them.
>
> #   PART 1: ENTERING THE DESCRIPTION OF THE FANO PLANE
>
> pnam:=array(1..7): #The names of the points in the paper
>  pnam[1]:="a1": pnam[2]:="a2": pnam[3]:="a3":
>  pnam[4]:="b1": pnam[5]:="b2": pnam[6]:="b3":
>  pnam[7]:="c":
> lnam:=array(8..14): #Lines names in the paper;
>  lnam[8]:="u1": lnam[9]:="u2":
>  lnam[10]:="u3": lnam[11]:="v1":
>  lnam[12]:="v2": lnam[13]:="v3": lnam[14]:="w":
> line:=array(8..14): #The lines in the paper
>  line[7+1]:={2,3,3+1}: line[7+2]:={1,3,3+2}:
>  line[7+3]:={1,2,3+3}: line[7+3+1]:={1,3+1,7}:
> line[7+3+2]:={2,3+2,7}:line[7+3+3]:={3,3+3,7}:
>  line[7+7]:={3+1,3+2,3+3}: #Each line is a set of points;
>  #the program treats the points numbers while computing
>  #but uses their names, stored in pnam, when printing.
> L:=array(0..15): #The subspace lattice of the Fano plane
> for i from 1 to 7 do L[i]:={i} od:#
> for i from 8 to 14 do L[i]:=line[i] od: L[0]:={}: L[15]:={}:
> for i from 1 to 7 do L[15]:=L[15] union {i} od:#
> lnotat:=array(0..15):
>  #The notations of the subspaces in the paper
>  #like "0", "a1", "u2", or "1".
>  lnotat[0]:="0":lnotat[15]:="1":
>  for i from 1 to 7 do lnotat[i]:=pnam[i] od:
>  for i from 8 to 14 do lnotat[i]:=lnam[i] od:
> leq:=proc(x,y) local r; #Describing the order
>   if x=x intersect y then r:=1 else r:=0 fi
> end:#
> SetToName:=proc(x) local i,r; #Name: what the paper uses
>  #E.g., SetToName=({2,4,3}) = "u1"
>  r:="Non-recognizable":
>  for i from 0 to 15 do if x=L[i] then r:=lnotat[i] fi
>  od:  r:=r:
> end: #End of SetToName
> SetToStr:=proc(x)
>  #E.g., SetToStr({2,3,4})="{a2,a3,b1}"
>  local i,r,needscomma;
>  r:="{": needscomma:=0:
>  for i from 1 to 7 do
```

```
>   if leq(L[i],x)=1 then
>     if needscomma=1 then r:=cat(r,",",lnotat[i])
>     else r:=cat(r,lnotat[i]): needscomma:=1
>     fi:
>   fi:
>  od: #end of "for i" loop
>  r:=cat(r,"}"):
> end: #End of procedure SetToStr
>
> #           PART 2: LISTING THE DETAILS OF THE FANO PLANE
>
> lstr:=array(0..15):#The subspaces in string forms
>  # like  "u1={a2,a2,b1}", "a1={a1}",  or "0={}"
>  for i from 0 to 15 do
>   lstr[i]:=cat(lnotat[i],"=",SetToStr(L[i]))
>  od:  #end of the "for i" loop
print("The details of the subspace lattice L"):
print("  of the Fano plane are as follows:"):
for i from 0 to 15 do print(cat(lstr[i],
                  " (stored in L(",i,")")) od:
                "The details of the subspace lattice L"
                 "  of the Fano plane are as follows:"
                        "0={} (stored in L(0)"
                      "a1={a1} (stored in L(1)"
                      "a2={a2} (stored in L(2)"
                      "a3={a3} (stored in L(3)"
                      "b1={b1} (stored in L(4)"
                      "b2={b2} (stored in L(5)"
                      "b3={b3} (stored in L(6)"
                       "c={c} (stored in L(7)"
                    "u1={a2,a3,b1} (stored in L(8)"
                    "u2={a1,a3,b2} (stored in L(9)"
                    "u3={a1,a2,b3} (stored in L(10)"
                    "v1={a1,b1,c} (stored in L(11)"
                    "v2={a2,b2,c} (stored in L(12)"
                    "v3={a3,b3,c} (stored in L(13)"
                     "w={b1,b2,b3} (stored in L(14)"
              "1={a1,a2,a3,b1,b2,b3,c} (stored in L(15)"
> #
> #               PART 3: COMPUTING THE JOIN IN L
> #
> which:=proc(x) local i,r; # x is subspace
>  r:=-1; for i from 0 to 15 do if x=L[i] then r:=i fi od;
>  # if r=-1 then print(" !!! -1 means: NOT IN L !!!"): fi:
>  r:=r;
> end: #And now a few tests with "which":
> #The built-in operation "intersect" is good for meet.
> join:=proc(x,y) local z,i,r:
>  z:=L[15]: #The top element
>  for i from 0 to 14 do
>   if (leq(x,L[i])=1) and (leq(y,L[i])=1)
>      then z:=z intersect L[i]
>   fi
```

```
>  od: #End of the "for i" loop
>  r:=z:
> end: #End of procedure join
>
> # Test:  in the next two lines, we test some joins in L:
> #a:={1}:b:={2,4,3}: c:=join(a,b); print(cat
> #(SetToName(a)," join ",SetToName(b),"=",SetToName(c))):
>
>
> #       PART 4: SEARCH IN S
>
> S:=array(1..257,1..2):#The sublattice to be generated
> Ssize:=0: #At present, S is the emptyset
> whereInS:=proc(x,y) local r,i:
>                       #Finds an element of L^2 in S
>  r:=-1:
>  for i from 1 to Ssize do
>   if (x=S[i,1]) and (y=S[i,2]) then r:=i
>   fi:
>  od: r:=r:
> end: #End of procedure whereInS; it will be tested later.
>
> #       PART 5: COMPUTING WHAT S GENERATES
>
> generating:=proc()  local i,j,z1,z2,m1,m2,found,oldSize;
>     global S,Ssize;
>  #Computes what (S[1,1],S[1,2]), ... ,
>  # (S[Ssize,1],S[Size,2]) generates,  puts it into S,
>  # and increases Ssize
>  found:=true:
>  while found=true
>  do found:=false: oldSize:=Ssize:
>   for i from 1 to oldSize-1
>   do for j from i+1 to oldSize
>    do z1:=join(S[i,1],S[j,1]): z2:=join(S[i,2],S[j,2]):
>       m1:=S[i,1] intersect S[j,1]:
>       m2:=S[i,2] intersect S[j,2]:
>       if whereInS(z1,z2)=-1 then
>        found:=true: Ssize:=Ssize+1:
>        S[Ssize,1]:=z1: S[Ssize,2]:=z2:
>       fi: # New join added
>       if whereInS(m1,m2)=-1 then
>        found:=true: Ssize:=Ssize+1:
>        S[Ssize,1]:=m1: S[Ssize,2]:=m2:
>       fi: # New meet added
>    od: # for j
>   od: # for i
>  od: #while found; now S is the sublattice generated.
> end: #End of procedure generating;
> #it will be tested later, after initialization
>
> #      PART 6: CONVERTING A ROW OF S TO TEXT
>
```

```
> Sname:=proc(i) local i1,i2,r:#E.g, Sname(1)="(a1,a1)"
>  i1:=which(S[i,1]); i2:=which(S[i,2]);
>  if (i1=-1) or (i2=-1)
>  then print("Something is wrong here"): r:=""
>  else  r:=cat("(",lnotat[i1],",",lnotat[i2],")")
>  fi: r:=r:
> end: #End of proceture Sname, to be tested later.
> #
> #Test:    FIRST TEST (OPTIONAL)
>
> #Testing what 3 points on a line and a further point
> #generate; and testing Sname and whereInS, too.
> #for i from 1 to 4 do S[i,1]:=L[i]: S[i,2]:=L[i]:
> #od:  Ssize:=4: print(cat("The subset of L^2:")):
> #for i from 1 to Ssize do print(Sname(i)) od:
> #generating():
> #print(cat("generates the following ",
> #            Ssize,"-element sublattice:"));
> #for i from 1 to Ssize do print(Sname(i)) od:
> #print("(A whereInS-test:"):
> #print(cat(Sname(L[8]),"=",L[8]," it is the ",
> # whereInS(L[8],L[8]),"-th" )):
>
> #Test:    SECOND TEST (OPTIONAL)
> #Testing what 4 points in general position  generate
> #for i from 1 to 3 do S[i,1]:=L[i]: S[i,2]:=L[i]:
> #od:  S[4,1]:=L[7]: S[4,2]:=L[7]: Ssize:=4: generating():
> #print(cat("The following ",Ssize,
> #                   "-element sublattice is generated",
> #      " by its first four elements:"));
> #for i from 1 to Ssize do print(Sname(i)) od:
>
> #      PART 7: THE MAIN COMPUTATION
> #
> for i from 1 to 3 do S[i,1]:=L[i]: S[i,2]:=L[i]:
> od:  S[4,1]:=L[7]: S[4,2]:=L[14]: Ssize:=4:
> print("The following 4 elements of L^2:"):
> txt:=Sname(1):for i from 2 to Ssize do
>             txt:=cat(txt,", ", Sname(i)) od: print(txt):
> generating():print("generate a ",
> Ssize,"-element sublattice,"):
> print("which consists of the following elements:"):
for i from 1 by 5 to Ssize do  txt="":
 for j from 0 to 4 do
  if i+j<Ssize  then txt:=cat(txt,Sname(i+j),", "):
  fi:
  if i+j=Ssize then txt:=cat(txt,Sname(i+j),"."):
  fi
 od: print(txt):
od:
a1:=lnotat[15]: a2:=lnotat[0]:
print(cat("The position of (", a1, ",", a2,
                  ") is ",whereInS(L[15],L[0]))):
```

```
print("(-1  means that not found)"):
                  "The following 4 elements of L^2:"
                  "(a1,a1), (a2,a2), (a3,a3), (c,w)"
              "generate a ", 50, "-element sublattice,"
            "which consists of the following elements:"
            "(a1,a1), (a2,a2), (a3,a3), (c,w), (u3,u3), "
             "(0,0), (u2,u2), (v1,1), (u1,u1), (v2,1), "
              "(v3,1), (1,1), (0,a1), (0,a2), (0,a3), "
             "(0,b3), (0,b2), (0,b1), (a1,u3), (a2,u3), "
          "(b3,u3), (a1,u2), (b2,u2), (a3,u2), (b1,u1), "
            "(c,1), (a2,u1), (a3,u1), (a1,v1), (u3,1), "
            "(u2,1), (a2,v2), (u1,1), (a3,v3), (0,u3), "
             "(0,u2), (0,u1), (0,v1), (b1,1), (a2,1), "
             "(a3,1), (0,v2), (a1,1), (b2,1), (0,v3), "
               "(b3,1), (0,w), (w,1), (0,1), (0,c)."
                   "The position of (1,0) is -1"
                    "(-1  means that not found)"
```

This program (called "worksheet" in Maple) is also available from the author's website.

References

[1] Artmann, B.: On coordinates in modular lattices with a homogeneous basis. Illinois J. Math. **12**, 626–648 (1968)

[2] Czédli, G.: Four-generated quasiorder lattices and their atoms in a four generated sublattice. Communications in Algebra **45** 4037–4049 (2017)

[3] Czédli, G.: Generating Boolean lattices by few elements and exchanging session keys. arXiv:2303.10790

[4] Czédli, G., Skublics, B.: The ring of an outer von Neumann frame in modular lattices. Algebra Universalis **64** 187–202 (2010)

[5] Day, A., Pickering, D.: The coordinatization of Arguesian lattices. Trans. Amer. Math. Soc. **278**, 507–522 (1983)

[6] Freese, R: The variety of modular lattices is not generated by its finite members. Trans. Amer. Math. Soc. **255**, 277–300 (1979)

[7] Gelfand, I.M., Ponomarev, V.A.: Problems of linear algebra and classification of quadruples of subspaces in a finite dimensional vector space. Hilbert Space Operators, Coll. Math. Soc. J. Bolyai 5, Tihany, Hungary (1970)

[8] Grätzer, G.: Lattice Theory: Foundation. Birkhäuser, Basel (2011)

[9] Herrmann, C.: On the equational theory of modular lattices. Proc. Univ. of Houston Lattice Theory Conference, Houston, 105–118 (1973)

[10] Herrmann, C.: On the arithmetic of projective coordinate systems. Trans. Amer. Math. Soc. **284**, 759–785 (1984)

[11] Herrmann, C., Huhn, A.P.: Lattices of normal subgroups which are generated by frames. Colloq. Math. Soc. J. Bolyai 14. Lattice Theory, Szeged (Hungary), 97–136 (1974)

[12] Huhn, A.P.: Schwach distributive Verbände I. Acta Sci. Math. (Szeged) **33**, 297–305 (1972) (in German)

[13] Milne, J.S.: Fields and Galois Theory. Kea Books[14], Ann Arbor (2022)

[14] von Neumann, J.: Algebraic theory of continuous geometries. Proc. Nat. Acad. Sci. U.S.A. **23**, 16–22 (1937)

[15] von Neumann, J.: Continuous Geometry. (Foreword by Israel Halperin), Princeton University Press, Princeton (1960)

[16] O'Hara, K.M.: Unimodality of Gaussian Coefficients: A Constructive Proof. Journal of Combinatorial Theory A **53**, 29–52 (1990)

[14]See also https://www.jmilne.org/math/CourseNotes/FT.pdf for an earlier version.

[17] Strietz, H.: Über Erzeugendenmengen endlicher Partitionverbände. Studia Sci. Math. Hungarica **12**, 1–17 (1977) (in German)
[18] Vanstone, S.A., van Oorschot, P.C.: An Introduction to Error Correcting Codes with Applications. Kluwer, Boston–Dordrecht–London (1989)
[19] Veblen, O., Young, J.W.: Projective Geometry I. Ginn and Co., Boston (1910)
[20] Wild, M.: Cover-preserving embedding of modular lattices into partition lattices. Discrete Mathematics **112**, 207–244 (1993)
[21] Wille, R.: On free modular lattices generated by finite chains. Algebra Universalis **3**, 131–138 (1973)
[22] Zádori, L.: Subspace lattices of finite vector spaces are 5-generated. Acta Sci. Math. (Szeged) 74 (2008), 493–499.

Email address: czedli@math.u-szeged.hu
URL: http://www.math.u-szeged.hu/~czedli/

University of Szeged, Bolyai Institute. Szeged, Aradi vértanúk tere 1, HUNGARY 6720