TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 251, July 1979

PROJECTIVE GEOMETRIES AS PROJECTIVE MODULAR LATTICES

BY
RALPH FREESE[1]

ABSTRACT. It is shown that the lattice of subspaces of a finite dimensional vector space over a finite prime field is projective in the class of modular lattices provided the dimension is at least 4.

In this paper it is shown that the lattice of subspaces of an n-dimensional vector space over the field with p elements (i.e., a projective geometry of dimension $n - 1$ over $\mathbf{Z}_p$) is a projective modular lattice for $4 \leqslant n < \omega$ and p a prime. This answers problem 9 of [15].

Recall that a modular lattice L is a *projective modular lattice* if for any modular lattices M and N and any lattice homomorphisms h of L into N and f of M onto N, there is a homomorphism g of L into M such that $f(g(a)) = h(a)$ for all $a \in L$. This is equivalent to the existence of a homomorphism f of a free modular lattice $\mathrm{FM}(X)$ onto L and a homomorphism g of L to $\mathrm{FM}(X)$ such that $f(g(a)) = a$ for all $a \in L$. The map $g \circ f$ is a *retraction*, i.e., it is an endomorphism of $\mathrm{FM}(X)$ which is point-wise fixed on its image. Thus projective modular lattices are the retracts (images of retractions) of free modular lattices. In particular, every projective modular lattice is a sublattice of a free modular lattice. Thus as a corollary to our result we obtain that every finite planar modular lattice can be embedded into a free modular lattice (in fact, into FM(4)), since all these lattices can be embedded into the subspace lattices described above (cf. [3]).

The first section of this paper reviews the definition and important results on von Neumann n-frames of characteristic r. It is shown in [4] the free modular lattice generated by an n-frame of characteristic r, which we denote $\mathrm{FM}(P(n, r))$, is a projective modular lattice for $3 \leqslant n < \omega$ and $r \geqslant 1$. In the second section a review of von Neumann's coordinatization is given. We prove the main result in the third section by showing that $\mathrm{FM}(P(n, p))$ is isomorphic to the lattice of subspaces of an n-dimensional vector space over $\mathbf{Z}_p$, for $4 \leqslant n < \omega$ and p a prime.

A subdirectly irreducible modular lattice L is a *splitting modular lattice* if there is a lattice equation ε such that each variety of modular lattices either

Received by the editors June 23, 1978.

AMS (MOS) subject classifications (1970). Primary 06A30.

[1] This work was partially supported by NSF Grant No. MCS77-01933.

satisfies ε or contains L, but not both (cf. [13]). The above results imply that the lattice of subspaces of an n-dimensional vector space over $\mathbf{Z}_p$, $L(\mathbf{Z}_p^n)$, is a splitting modular lattice (see [2]). Moreover, the Hall-Dilworth example of the second kind obtained by gluing $L(\mathbf{Z}_p^4)$ and $L(\mathbf{Z}_q^4)$ together over a one-dimensional quotient is a splitting modular lattice. Let ε_{pq} be the splitting equation. In a subsequent paper this will be applied to congruence varieties. It will be shown that if $\mathcal{K}$ is a variety of algebras with modular congruence lattices, then those congruence lattices satisfy ε_{pq}, $p \neq q$. Thus congruence modularity implies identities strictly stronger than the arguesian law (cf. [5]).

1. Preliminaries. Let L be a modular lattice. We say that L contains an n-frame if there exist $a_1, \ldots, a_n, c_{12}, c_{13}, \ldots, c_{1n} \in L$ such that (i) the sublattice generated by $a_1, \ldots, a_n$ is the Boolean algebra $\mathbf{2}^n$ with atoms $a_1, \ldots, a_n$, and (ii) $a_1 + c_{1j} = a_j + c_{1j} = a_1 + a_j$ and $a_1 c_{1j} = a_j c_{1j} = a_1 a_j$. In this situation we shall simply say that $\{a_i, c_{1j}\}$ is an n-frame in L. We let 0 denote the least element of this Boolean algebra, i.e., $0 = a_1 a_2$ and we do not insist that 0 is the least element of L. We let $P(n)$ denote an n-frame as an abstract system of generators and relations and we let $\mathrm{FM}(P(n))$ be the modular lattice freely generated by $a_1, \ldots, a_n, c_{12}, \ldots, c_{1n}$ subject to the relations described above which make $\{a_1, \ldots, a_n, c_{12}, \ldots, c_{1n}\}$ an n-frame. A great deal of information about n-frames is contained in [9]–[12], [14].

Let $\{a_i, c_{1j};\ i = 1, \ldots, n, j = 2, \ldots, n\}$ be an n-frame in a modular lattice L. Let $c_{j1} = c_{1j}$ and for 1, i, j distinct let $c_{ij} = (c_{1i} + c_{1j})(a_i + a_j)$. In Lemma 5.3 of [14, p. 118], it is shown that, for distinct i, j, k,

$$c_{ik} = (c_{ij} + c_{jk})(a_i + a_k). \tag{1.1}$$

In the definition of an n-frame the index 1 plays a special role. However, by (1.1), we see that this apparent lack of symmetry is only illusionary.

Let $\{a_i, c_{1j}\}$ be an n-frame in a modular lattice L, $n \geq 3$. Then for i, j, k distinct we have the following projectivity

$$\begin{aligned} a_i + a_j/0 \nearrow a_i + a_j + a_k/a_k &\searrow c_{ik} + a_j/0 \\ \nearrow a_i + a_j + a_k/c_{jk} &\searrow a_i + a_j/0. \end{aligned} \tag{1.2}$$

This projectivity defines an automorphism α_{ij} of $a_i + a_j/0$ given by

$$\alpha_{ij}(x) = ((x + a_k)(c_{ik} + a_j) + c_{jk})(a_i + a_j). \tag{1.3}$$

If $\{a_i, c_{1j}\}$ is an n-frame, $n \geq 3$, in a modular lattice L and r is a positive integer, we say that it is an n-frame of characteristic r if

$$\alpha_{12}^r(a_1) = a_1. \tag{1.4}$$

Here α_{12}^r is α_{12} iterated r times. We let $P(n, r)$ denote an n-frame of characteristic r as an abstract system of generators and relations, and we let $\mathrm{FM}(P(n, r))$ denote the modular lattice freely generated by $P(n, r)$. That is,

$\mathrm{FM}(P(n, r))$ is the modular lattice freely generated by $a_1, \ldots, a_n, c_{12}, \ldots, c_{1n}$ subject to the relations which make it an n-frame and the additional relation (1.4).

It is shown in Theorem 1.6 of [4] that if f is a homomorphism from a modular lattice M onto L and L contains an n-frame $\{a_i, c_{1j}\}$ of characteristic r, then M contains an n-frame $\{\bar{a}_i, \bar{c}_{1j}\}$ of characteristic r such that $f(\bar{a}_i) = a_i$ and $f(\bar{c}_{1j}) = c_{1j}$. The next theorem follows from this and the definition of $\mathrm{FM}(P(n, r))$.

THEOREM 1.1. *For $n \geqslant 3$ and r a positive integer,* $\mathrm{FM}(P(n, r))$ *is a projective modular lattice.*

2. A review of von Neumann's coordinatization. We shall require some of von Neumann's results on coordinatizing modular lattices, **[14]**, **[7]**, **[12]**. Von Neumann begins with a complemented modular lattice L containing an n-frame, $n \geqslant 4$, and uses this n-frame to define a ring with 1, R_L, called the *auxiliary ring*. He then uses R_L to coordinatize L. In defining R_L and showing that it is a ring von Neumann does not use the hypothesis that L is complemented. Thus every modular lattice that contains an n-frame, $n \geqslant 4$, has an auxiliary ring R_L (which depends on the n-frame as well as L). Let $\{a_i: i = 1, \ldots, n\} \cup \{c_{1j}: j = 2, \ldots, n\}$ be an n-frame in L. Let

$$L_{ij} = \{x \in L\colon xa_j = 0 \text{ and } x + a_j = a_i + a_j\}.$$

Here $0 = a_1a_2$ and need not be the least element of L. Let i, j, k be distinct. Since

$$a_i + a_j/0 \nearrow a_i + a_j + a_k/c_{ik} \searrow a_k + a_j/0,$$

there is a projective isomorphism

$$P\binom{i\ j}{k\ j}\colon a_i + a_j/0 \rightarrow a_k + a_j/0 \tag{2.1}$$

given by

$$x \mapsto (x + c_{ik})(a_k + a_j). \tag{2.2}$$

Similarly we have

$$P\binom{i\ j}{i\ h}\colon a_i + a_j/0 \rightarrow a_i + a_h/0, \tag{2.3}$$

$$x \mapsto (x + c_{jh})(a_i + a_h).$$

If i, j, k, h are distinct, set

$$P\binom{i\ j}{k\ h} = P\binom{i\ j}{k\ j} \circ P\binom{k\ j}{k\ h}.$$

An *L-number* is an ordered $n(n - 1)$-tuple

$$\beta = (\beta_{ij}\colon i \neq j, i, j = 1, \ldots, n)$$

such that

$$\beta_{ij} \in L_{ij}, \tag{2.4}$$

$$\beta_{kh} = \beta_{ij} P\binom{i\ j}{k\ h} \quad \text{all } i \neq j, \quad k \neq h. \tag{2.5}$$

By (2.5) an L-number is determined by any one of its components. Conversely we have the following.

LEMMA 2.1 ([**14**, p. 130]). *If $b_{ij} \in L_{ij}$, then there is a unique L-number β whose (i, j)th component is b_{ij}.*

Suppose β, γ are L-numbers and that i, j, k are distinct indices. Set

$$\delta_{ik} = (\beta_{ij} + \gamma_{jk})(a_i + a_k). \tag{2.6}$$

von Neumann shows that $\delta_{ik} \in L_{ik}$ and thus uniquely determines an L-number δ by Lemma 2.1. Moreover he shows that the L-number thus obtained is independent of the choice of i, j, k [**14**, p. 131], and (2.6) holds for all choices of distinct i, j, k. Multiplication of L-numbers is now defined by $\gamma\beta = \delta$ (cf. [**7**, p. 289]).

If β and γ are L-numbers, then the sum is the L-number δ whose (i, j)th component is given by

$$\delta_{ij} = \left[(\beta_{ij} + c_{ik})(a_j + a_k) + (\gamma_{ij} + a_k)(a_j + c_{ik})\right](a_i + a_j). \tag{2.7}$$

Furthermore, von Neumann shows that if L-numbers β, γ, δ satisfy (2.7) for one distinct triple i, j, k, they satisfy it for all such triples. In particular the above formula for δ_{ij} is independent of the choice of $k \neq i,j$. Using this we obtain additional independence in the definition of addition.

LEMMA 2.2. *If $\beta_{ij}, \gamma_{ij} \in L_{ij}$ and $c'_{ik} \in L_{ik} \cap L_{ki}$, then*

$$\begin{aligned}&\left[(\beta_{ij} + c_{ik})(a_j + a_k) + (\gamma_{ij} + a_k)(a_j + c_{ik})\right](a_i + a_j)\\ &\qquad = \left[(\beta_{ij} + c'_{ik})(a_j + a_k) + (\gamma_{ij} + a_k)(a_j + c'_{ik})\right](a_i + a_j).\end{aligned} \tag{2.8}$$

PROOF. Define $a'_l = a_l$, $l = 1, \ldots, n$, $c'_{il} = c_{il}$ for $l \neq i, k$, and let c'_{ik} be the element given in the lemma. For $i \neq h,l$ let

$$c'_{hl} = c'_{lh} = (c'_{ih} + c'_{il})(a'_h + a'_l).$$

Using Lemma 5.3 [**14**, p. 118], the reader can show that $\{a'_l, c'_{1l}\}$ forms an n-frame. Since $n \geqslant 4$, choose $l \neq i,j,k$. By the above remarks the left side of (2.8) is unchanged if k is replaced by l and the right side also unchanged if k is replaced by l. But since $c'_{il} = c_{il}$, the resulting expressions are equal. Hence (2.8) holds. □

With the above operations the L-numbers form a ring R_L with 1 [**14**, p. 157]. The 1 of this ring is the L-number whose (i,j)th coordinate is c_{ij} and whose 0 is the L-number whose (i,j)th coordinate is a_i. We let 1 and 0 denote these L-numbers so that $(1)_{ij} = c_{ij}$ and $(0)_{ij} = a_i$. (1 and 0 also denote the greatest and least elements of the n-frame; no confusion should arise.)

At this point we take $L = \mathrm{FM}(P(n,p))$, where $n \geq 4$ and p is a prime. Let α_{ij} be the automorphism of $a_1 + a_2/0$ given by (1.3), and let β be an L-number. Checking the definition of $1 \oplus \beta$ (we use $\oplus$ for the addition in R_L) and comparing it with the definition of α_{ij} we see that $(1 \oplus \beta)_{ij} = \alpha_{ij}(\beta_{ij})$. Since $\alpha_{12}^p(a_1) = a_1$ holds in $L = \mathrm{FM}(P(n,p))$ by definition,

$$0 \oplus 1 \oplus 1 \oplus \cdots \oplus 1 = 0 \qquad (p \text{ 1's})$$

holds in R_L. Thus R_L has characteristic p. Consequently there is an embedding of $\mathbf{Z}_p$ into R_L given by

$$t \mapsto \left(\alpha_{ij}^t(a_i)\colon 1 \leq i,j \leq n, i \neq j\right), \qquad t = 0,1,\ldots,p-1. \tag{2.9}$$

For $t \in \mathbf{Z}$ or $\mathbf{Z}_p$ we abbreviate the L-number $(\alpha_{ij}^t(a_i)\colon 1 \leq i,j \leq n, i \neq j)$ by t. Thus $t_{ij} = \alpha_{ij}^t(a_i)$. Formula (2.6) for multiplication yields for $r,s \in \mathbf{Z}_p$

$$(r_{ij} + s_{jk})(a_i + a_k) = (rs)_{ik}. \tag{2.10}$$

Lemma 2.3. *An L-number β has a two-sided multiplicative inverse if and only if $\beta_{ij} \in L_{ji}$ for some (and hence for all) $i \neq j$. If γ is the inverse of β, then $\gamma_{ij} = \beta_{ji}$ for all $i \neq j$.*

Proof. Let γ be an L-number such that $\gamma\beta = \beta\gamma = 1$. Then, by (2.6),

$$c_{ji} = c_{ij} = (\beta_{ik} + \gamma_{kj})(a_i + a_j).$$

Thus

$$c_{ji} + \beta_{ik} = (\beta_{ik} + \gamma_{kj})(a_i + a_j + \beta_{ik})$$

and

$$\begin{aligned}
\beta_{jk} &= (c_{ji} + \beta_{ik})(a_j + a_k)\\
&= (\beta_{ik} + \gamma_{kj})(a_j + a_k)(a_i + a_j + \beta_{ik})\\
&= (\gamma_{kj} + \beta_{ik}(a_j + a_k))(a_i + a_j + \beta_{ik})\\
&= (\gamma_{kj} + \beta_{ik}(a_i + a_k)(a_j + a_k))(a_i + a_j + \beta_{ik})\\
&= (\gamma_{kj} + \beta_{ik}a_k)(a_i + a_j + \beta_{ik})\\
&= \gamma_{kj}(a_i + a_j + \beta_{ik})\\
&\leq \gamma_{kj}.
\end{aligned}$$

A similar argument gives $\gamma_{kj} \leq \beta_{jk}$. Thus $\beta_{jk} = \gamma_{kj} \in L_{kj}$. A proof of the converse is given in Anmerkung 3.1 of [**12**, p. 208]. □

If $r \not\equiv 0 \pmod{p}$, it is invertible in $\mathbf{Z}_p$ and hence R_L. As a corollary, we obtain the following formula, which will be used later.

$$(1/r)_{ij} = (r)_{ji} \quad \text{for } r \not\equiv 0 \pmod{p}. \tag{2.11}$$

Here $1/r$ is the inverse of r in $\mathbf{Z}_p$. (Recall that $r_{ji} = \alpha_{ji}^r(a_j)$, etc.)

Lemma 2.4. *Let i, j, k be distinct and β, γ be L-numbers. Then*

$$(a_k + \beta_{ij})(a_i + \gamma_{jk}) = (a_k + \beta_{ij})(a_j + (-\gamma\beta)_{ik}).$$

Proof. This is Lemma 10.6 of [**14**, p. 172]. Although at this point, von Neumann has begun to use complemention, this lemma does not require it. □

3. The main result. In this section we prove the following theorem.

Theorem 3.1. *Let V be a vector space of dimension n, $4 < n < \omega$, over $\mathbf{Z}_p$, p a prime. Let $L(V)$ be its lattice of subspaces. Then $L(V)$ is a projective modular lattice.*

By Theorem 1.1, the above result will follow from the next theorem.

Theorem 3.2. *Let V be as above. Then $L(V) \cong \mathrm{FM}(P(n,p))$.*

Proof. We take V to be n-tuples of elements from $\mathbf{Z}_p$. If $v = (v_1, \ldots, v_n) \in V$, we define the *support* of v to be $\{i \colon v_i \neq 0\}$. If $v \in V$, let $v^{(i)}$ be the vector obtained from v by setting the ith component equal to 0. Throughout this section we let $L = \mathrm{FM}(P(n,p))$.

Define a map $c \colon V \to L$ by

$$c(0) = 0, \tag{3.1}$$

$$c(0, \ldots, 0, r, 0, \ldots, 0) = a_i \quad \text{if } r \neq 0, \quad r \in \mathbf{Z}_p, \tag{3.2}$$

where r is in the ith place,

$$c(0, \ldots, r, \ldots, s, \ldots, 0) = (-s/r)_{ij}, \qquad r,s \in \mathbf{Z}_p, \quad r \neq 0, \tag{3.3}$$

where r and s are in the ith and jth places, respectively, and inductively if the support of v has at least three elements, i and j among them, define

$$c(v) = \big(a_i + c(v^{(i)})\big)\big(a_j + c(v^{(j)})\big). \tag{3.4}$$

Recall that $(-s/r)_{ij} = \alpha_{ij}^{-s/r}(a_i) = \alpha_{ij}^t(a_i)$ where t is an integer such that $-s \equiv tr \pmod{p}$. Since $\alpha_{ij}^p(a_i) = a_i$, $\alpha_{ij}^t(a_i)$ does not depend on which t is chosen. By equation (2.11), $(-s/r)_{ij} = (-r/s)_{ji}$ if $s \neq 0$ in $\mathbf{Z}_p$. Thus (3.3) is well defined.

We shall now show that (3.4) is independent of the choice of i and j in the support of v. First suppose that the support of v is exactly $\{i, j, k\}$ and that $v_i = r_i$, $v_j = r_j$, and $v_k = r_k$, with r_i, r_j, r_k all nonzero in $\mathbf{Z}_p$. Since i and k are in the support of v,

$$c(v) = \big(a_i + c(v^{(i)})\big)\big(a_k + c(v^{(k)})\big).$$

Now $c(v^{(i)}) = (-r_k/r_j)_{jk}$ and $c(v^{(k)}) = (-r_j/r_i)_{ij}$ by (3.3). Thus, since

$$-(-r_k/r_j)(-r_j/r_i) = -r_k/r_i,$$

Lemma 2.4 yields

$$\begin{aligned} c(v) &= (a_i + (-r_k/r_j)_{ji})(a_k + (-r_j/r_i)_{ij}) \\ &= (a_k + (-r_j/r_i)_{ij})(a_j + (-r_k/r_i)_{ik}). \end{aligned}$$

Proceeding by induction, assume that the support of v contains at least four indices and that i, j, k are among them. We abbreviate the vector $(v^{(i)})^{(j)}$ by $v^{(i,j)}$. It suffices to show that

$$(a_i + c(v^{(i)}))(a_j + c(v^{(j)})) < a_k + c(v^{(k)}).$$

Since (3.4) holds for $v^{(i)}$, $c(v^{(i)}) < a_k + c(v^{(i,k)})$. Thus

$$a_i + c(v^{(i)}) < a_i + a_k + c(v^{(i,k)})$$

and

$$a_j + c(v^{(j)}) < a_j + a_k + c(v^{(j,k)}).$$

Let S be the support of v. The reader can show by induction that

$$a_i + c(v^{(i,k)}) < \Sigma(a_h \colon h \in S, h \neq k).$$

Thus

$$\begin{aligned} (a_i + c(v^{(i)}))(a_j + c(v^{(j)})) &< (a_i + a_k + c(v^{(i,k)}))(a_j + a_k + c(v^{(j,k)})) \\ &= a_k + (a_i + c(v^{(i,k)}))\Bigg(\sum_{\substack{h \in S \\ h \neq k}} a_h\Bigg)(a_j + a_k + c(v^{(j,k)})) \\ &= a_k + (a_i + c(v^{(i,k)}))\Big(a_j + c(v^{(j,k)}) + a_k \sum_{h \neq k} a_h\Big) \\ &= a_k + (a_i + c(v^{(i,k)}))(a_j + c(v^{(j,k)})) \\ &= a_k + c(v^{(k)}). \end{aligned}$$

Lemma 3.3. (i) *If i is in the support of $v \in V$, then $a_i + c(v) = a_i + c(v^{(i)})$.*

(ii) *If $u, v \in V$ and $u_i \neq 0 \neq v_i$ and $v_j = u_j$ for all j except possibly i, then $a_i + c(u) = a_i + c(v)$.*

(iii) *If $r \neq 0$ in $\mathbf{Z}_p$, then $c(rv) = c(v)$.*

Proof. (i) If (3.2) applies to v, then (i) holds. If (3.3) applies with $s \neq 0$, then

$$\begin{aligned} a_i + c(v) &= a_i + (-s/r)_{ij} = a_i + (-r/s)_{ji} \\ &= a_i + a_j = a_i + c(v^{(i)}), \end{aligned}$$

since $(-r/s)_{ji} \in L_{ji}$.

Now suppose v has support with at least three elements, with i and j among them. Then by induction $a_i + c(v^{(j)}) = a_i + c(v^{(i,j)})$ and by definition $c(v^{(i)}) < a_j + c(v^{(i,j)})$. Thus, by (3.4),

$$\begin{aligned} a_i + c(v) &= a_i + \big(a_i + c(v^{(i)})\big)\big(a_j + c(v^{(j)})\big) \\ &= \big(a_i + c(v^{(i)})\big)\big(a_i + a_j + c(v^{(j)})\big) \\ &= \big(a_i + c(v^{(i)})\big)\big(a_i + a_j + c(v^{(i,j)})\big) \\ &= a_i + c(v^{(i)}). \end{aligned}$$

Part (ii) of the lemma follows immediately from part (i). Part (iii) follows easily from the definition of c. □

Part (iii) of the above lemma shows that c may be viewed as a map from the one-dimensional subspaces of V into L. We wish to extend c to all of $L(V)$. First we require some knowledge of the automorphisms of $L = \mathrm{FM}(P(n,p))$.

Recall that $\mathrm{GL}(n,p)$, the general linear group of degree n over $\mathbf{Z}_p$, is the group of all nonsingular $n \times n$ matrices with entries in $\mathbf{Z}_p$. We wish to show that $\mathrm{GL}(n,p)$ can act on $\mathrm{FM}(P(n,p))$ as a group of automorphisms. Recall that $n > 4$. Let $E_{r(i)}$ be the element of $\mathrm{GL}(n,p)$ obtained from the identity matrix by multiplying the ith row by r, $r \in \mathbf{Z}_p$, $r \neq 0$, $i = 1, \ldots, n$. Let $E_{(i)(j)}$ be the matrix obtained from the identity by interchanging the ith and jth rows. For $i \neq j$ let $E_{(i)+r(j)}$ be the matrix whose main diagonal entries are all 1 and whose (i,j)th entry is r and whose other entries are all 0. These matrices are called elementary matrices.

LEMMA 3.4. *$\mathrm{GL}(n,p)$ is generated by $E_{(1)(j)}$, $j = 2, \ldots, n$, $E_{r(4)}$, $r \in \mathbf{Z}_p - \{0\}$, $E_{(3)-r(4)}$, $r \in \mathbf{Z}_p$.*

PROOF. Since the symmetric group on $\{1, 2, \ldots, n\}$ is generated by transpositions of the form $(1,j)$, the $E_{(1)(j)}$ generate all permutation matrices. Now $E_{r(i)} = PE_{r(4)}P^{-1}$ where $P = E_{(4)(i)}$ and $E_{(i)-r(j)} = PE_{3-r(4)}P^{-1}$ where $P = E_{(4)(j)}E_{(3)(i)}$. Thus we obtain all the elementary matrices and these are known to generate $\mathrm{GL}(n,p)$. □

Consider the result of letting $E_{(3)-r(4)}$ act on

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \qquad (1 \text{ in the } i\text{th place})$$

and

$$e_{1j} = (-1, 0, \ldots, 0, 1, 0, \ldots, 0) \qquad (1 \text{ in the } j\text{th place}).$$

e_4 is mapped to $(0, 0, -r, 1, \ldots)$ and the other e_i are fixed. e_{14} is mapped to $(-1, 0, -r, 1, \ldots)$. In analogy to this we define

$$a'_4 = r_{43} = \alpha^r_{43}(a_4), \qquad a'_i = a_i \quad \text{for } i \neq 4,$$

$$c'_{14} = (a_1 + r_{43})(a_3 + c_{14}), \qquad c'_{1j} = c_{1j}, \quad j \neq 4$$

(cf. (3.3) and (3.4)).

LEMMA 3.5. *The $\{a'_i, c'_{1j}\}$ defined above form an n-frame of characteristic p.*

PROOF. Since $a'_4 = r_{43} < a_3 + a_4$, $a'_i(\Sigma_{j \neq i} a'_j) = 0$ if $i \neq 3$ or 4. Moreover

$$a'_3\Big(\sum_{j \neq 3} a'_j\Big) = a_3(a_3 + a_4)(a_1 + a_2 + r_{43} + \cdots) = a_3 r_{43} = 0$$

and

$$a'_4\Big(\sum_{j \neq 4} a'_j\Big) = r_{43}\Big(\sum_{j \neq 4} a_j\Big) = r_{43}(a_3 + a_4)\Big(\sum_{j \neq 4} a_j\Big) = r_{43}a_3 = 0.$$

Hence $a'_1, \ldots, a'_n$ are independent.

Now we shall show that a'_1, c'_{14}, a'_4 generate a copy of M_3:

$$\begin{aligned}
a'_1 c'_{14} &= a_1(a_3 + c_{14}) = 0, \\
a'_4 c'_{14} &= r_{43}(a_3 + c_{14}) = r_{43}(a_3 + a_4)(a_3 + c_{14}) = r_{43}a_3 = 0, \\
a'_1 + c'_{14} &= a_1 + (a_1 + r_{43})(a_3 + c_{14}) \\
&= (a_1 + r_{43})(a_1 + a_3 + c_{14}) \\
&= a_1 + r_{43} = a'_1 + a'_4, \\
a'_4 + c'_{14} &= r_{43} + (a_1 + r_{43})(a_3 + c_{14}) \\
&= (a_1 + r_{43})(r_{43} + a_3 + c_{14}) \\
&= (a_1 + r_{43})(a_1 + a_3 + a_4) \\
&= a_1 + r_{43} = a'_1 + a'_4.
\end{aligned}$$

Thus $\{a'_i, c'_{1j}\}$ is an n-frame. Let α'_{12} be defined as α_{12} using the primed elements. Notice

$$c'_{23} = (c'_{12} + c'_{13})(a'_2 + a'_3) = (c_{12} + c_{13})(a_2 + a_3) = c_{23}.$$

Now α'_{12} only uses the elements $a'_1, a'_2, a'_3, c'_{12}, c'_{13}, c'_{23}$. Since each of these elements is equal to the corresponding unprimed elements, $\alpha'_{12} = \alpha_{12}$. Thus $\alpha'^{p}_{12}(a'_1) = \alpha^{p}_{12}(a_1) = a_1 = a'_1$, i.e., the frame $\{a'_i, c'_{1j}\}$ has characteristic p. □

It follows from the defining properties of FM$(P(n, p))$ and from the above lemma that there is an endomorphism f of FM$(P(n, p))$ such that $f(a_i) = a'_i$ and $f(c_{1j}) = c'_{1j}$. Let $A = E_{(3)-r(4)}$.

LEMMA 3.6. *$f(c(v)) = c(Av)$ for all $v \in V$.*

PROOF. If $v_4 = 0$, then $Av = v$ and an easy induction shows that $f(c(v)) = c(v)$. Since if $s \neq 0$, $c(sv) = c(v)$ and $sAv = Asv$, we may assume $v_4 = 1$. If $v_i = 0$ for all i but 4, then $c(v) = a_4$, $f(c(v)) = a'_4$ and

$$c(Av) = c(0, 0, -r, 1, \ldots) = r_{43} = a'_4.$$

Now suppose $v = (0, 0, -s, 1, 0, \ldots)$. Then

$$c(v) = \alpha^{s}_{43}(a_4) = s_{43}, \qquad Av(0, 0, -r - s, 1, 0, \ldots).$$

Hence $c(Av) = \alpha_{43}^{s+r}(a_4) = (s + r)_{43}$. We shall show that $f(c(v)) = f(s_{43}) = (s + r)_{43} = c(Av)$ by induction on s. The case $s = 0$ was handled above. Assume the result for $s - 1$. First note that $a_3 + a_4' = a_3 + r_{43} = a_3 + a_4$ since $r_{43} \in L_{43}$ and

$$\begin{aligned} a_3 + c_{41}' &= a_3 + (a_1 + r_{43})(a_3 + c_{14}) \\ &= (a_3 + a_1 + r_{43})(a_3 + c_{14}) = a_3 + c_{14} = a_3 + c_{41}. \end{aligned}$$

Now using the addition formula (2.7) (recall $1_{ij} = c_{ij}$) and induction we obtain

$$\begin{aligned} f(c(v)) &= f(s_{43}) \\ &= f((c_{13} + ((s - 1)_{43} + a_1)(a_3 + c_{41}))(a_3 + a_4)) \\ &= (c_{13} + (f((s - 1)_{43}) + a_1)(a_3 + c_{41}))(a_3 + a_4) \\ &= (c_{13} + ((s + r - 1)_{43} + a_1)(a_3 + c_{41}))(a_3 + a_4) \\ &= (s + r)_{43}. \end{aligned}$$

In the case $s = 1$ we obtain $f(c_{43}) = (r + 1)_{43}$.

Now assume $v_4 = 1$ and $v_k = -s \neq 0$ and $v_j = 0$ for $j \neq 4,k$, where $k \neq 3,4$. Then

$$(Av)_3 = -r, \qquad (Av)_4 = 1, \qquad (Av)_k = -s,$$

and

$$(Av)_j = 0, \qquad j \neq 3,4,k.$$

By (3.4) and (3.3) and (2.6),

$$c(v) = s_{4k} = (c_{43} + s_{3k})(a_4 + a_k).$$

Thus

$$f(c(v)) = ((r + 1)_{43} + s_{3k})(r_{43} + a_k).$$

By Lemma 2.3, $s_{4k} \in L_{4k} \cap L_{k4}$. Thus we can apply Lemma 2.2 with $c_{ik}' = s_{4k}$ to obtain

$$(r + 1)_{43} = [(r_{43} + a_k)(s_{4k} + a_3) + (c_{43} + s_{4k})(a_3 + a_k)](a_3 + a_4).$$

Since $c_{43} = c_{34}$, $(c_{43} + s_{4k})(a_3 + a_k) = s_{3k}$. Thus

$$\begin{aligned} (r + 1)_{43} + s_{3k} &= [(r_{43} + a_k)(s_{4k} + a_3) + s_{3k}](a_3 + a_4 + s_{3k}) \\ &= ((r_{43} + a_k)(s_{4k} + a_3) + s_{3k})(a_3 + a_4 + a_k) \\ &= (r_{43} + a_k)(s_{4k} + a_3) + s_{3k}. \end{aligned}$$

Hence,

$$\begin{aligned} f(c(v)) &= ((r_{43} + a_k)(s_{4k} + a_3) + s_{3k})(r_{43} + a_k) \\ &= (r_{43} + a_k)(s_{4k} + a_3) + s_{3k}(r_{43} + a_k) \\ &= (r_{43} + a_k)(s_{4k} + a_3) = c(Av), \end{aligned}$$

since

$$\begin{aligned} s_{3k}(r_{43} + a_k) &= s_{3k}(a_3 + a_k)(r_{43}(a_3 + a_4) + a_k) \\ &= s_{3k}(a_k + a_3 r_{43}) = s_{3k}a_k = 0. \end{aligned}$$

Now let v be a vector with support at least three, i and j in the support, $i \neq j \neq 4 \neq i$. Now using induction

$$\begin{aligned} f(c(v)) &= f(a_i + c(v^{(i)}))(a_j + c(v^{(j)})) \\ &= (a_i + c(A(v^{(i)})))(a_j + c(A(v^{(j)}))) \end{aligned}$$

and, if $i,j \neq 3$,

$$c(Av) = (a_i + c((Av)^{(i)}))(a_j + c((Av)^{(j)})).$$

Furthermore for $\{i,j\} \cap \{3, 4\} = \varnothing$, $(Av)^{(i)} = A(v^{(i)})$, $(Av)^{(j)} = A(v^{(j)})$ and thus $f(c(v)) = c(Av)$. Assume now that $i = 3$. We can assume the support of v is 3, 4, and j for if there were another element in the support we would use that for i. If $(Av)_3 \neq 0$, then

$$c(Av) = (a_3 + c((Av)^{(3)}))(a_j + c((Av)^{(j)})).$$

By Lemma 3.3,

$$a_3 + c((Av)^{(3)}) = a_3 + c(Av) = a_3 + c(A(v^{(3)})).$$

Thus $f(c(v)) = c(A(v))$ holds in this case. In the one remaining case we have $v_4 = 1$, $v_3 = r$, $v_j = -s$ and $v_k = 0$ otherwise. Then $(Av)_3 = 0$ and Av agrees with v in the other coordinates. Thus $c(Av) = s_{4j}$. Now

$$\begin{aligned} f(c(v)) &= f((a_j + (-r)_{43})(s_{4j} + a_3)) \\ &= (a_j + a_4)(a_3 + (r_{43} + a_j)(s_{4j} + a_3)) \\ &= (a_j + a_4)(a_3 + a_j + r_{43})(s_{4j} + a_3) \\ &= (a_j + a_4)(a_3 + a_4 + a_j)(s_{4j} + a_3) \\ &= s_{4j} + (a_j + a_4)a_3 = s_{4j} = c(Av). \quad \square \end{aligned}$$

Let $r \in \mathbf{Z}_p$, $r \neq 0$ and let $B = E_{r(4)}$ so that $(Bv)_i = v_i$ for $i \neq 4$ and $(Bv)_4 = rv_4$. Define $a'_i = a_i$, $i = 1, \ldots, n$, and $c'_{1j} = c_{1j}$ if $j \neq 4$ and $c'_{14} = r_{14}$. Since $r \neq 0$, Lemma 2.3 implies that $r_{14} \in L_{41}$. From this it follows that $\{a'_i, c'_{1j}\}$ is an n-frame. Furthermore this n-frame has characteristic p since the elements defining $\alpha_{12}^{p}(a_1)$ are the same in the primed frame. Hence there is an endomorphism g of $\mathrm{FM}(P(n,p))$ such that $g(a_i) = a'_i$ and $g(c_{1j}) = c'_{1j}$.

LEMMA 3.7. *For all $v \in V$, $g(c(v)) = c(Bv)$.*

PROOF. If $v_4 = 0$, then it is easy to see that $g(c(v)) = c(v) = c(Bv)$. Thus, as above, we may assume $v_4 = 1$. If all the other components are zero, the result holds. Suppose $v_j = -s \neq 0$ and $v_k = 0$ if $k \neq 4,j$. Also suppose $j \neq 1$.

Then since $c_{41} = c_{14}$ and $r_{14} = (1/r)_{41}$, by (2.11),

$$\begin{aligned} g(c(v)) &= g(s_{4j}) \\ &= g(c_{41} + s_{1j})(a_4 + a_j) = (r_{14} + s_{1j})(a_4 + a_j) \\ &= ((1/r)_{41} + s_{1j})(a_4 + a_j) = (s/r)_{4j} = c(Bv). \end{aligned}$$

If $j = 1$, choose $k \neq 1,4$ then using the above,

$$\begin{aligned} g(c(v)) &= g(s_{41}) = g((s_{4k} + c_{k1})(a_4 + a_1)) \\ &= ((s/r)_{4k} + c_{k1})(a_4 + a_1) = (s/r)_{41} = c(Bv). \end{aligned}$$

Since $(Bv)^{(i)} = B(v^{(i)})$, the case when v has at least three nonzero components is easily handled. □

We now consider $E_{(1)(j)}$. We let $j = 2$; the other cases are similar. Let $C = E_{(1)(2)}$ and let $a_1' = a_2$, $a_2' = a_1$, $a_j' = a_j$, $j > 2$, $c_{12}' = c_{21} = c_{12}$, $c_{1j}' = c_{2j}$, $j > 2$. It is easy to check that $\{a_i', c_{1j}'\}$ is an n-frame of characteristic p. Let h be the endomorphism of $\mathrm{FM}(P(n,p))$ satisfying $h(a_i) = a_i'$, $h(c_{1j}) = c_{1j}'$.

Lemma 3.8. *For all $v \in V$, $h(c(v)) = c(Cv)$.*

Proof. The result holds if v has only one nonzero component. Suppose $v_1 = 1$ and $v_j = -s$ and $v_k = 0$ otherwise. Assume $j \neq 2$. Choose $k \neq 1,2,j$. Note that

$$\begin{aligned} h(c_{kj}) &= h((c_{1k} + c_{1j})(a_k + a_j)) \\ &= (c_{2k} + c_{2j})(a_k + a_j) = c_{kj}. \end{aligned}$$

For v as above, $c(v) = s_{1j}$. We shall show by induction that $h(s_{1j}) = s_{2j} = c(Cv)$:

$$\begin{aligned} h(s_{1j}) &= h((((s-1)_{1j} + a_k)(a_j + c_{1k}) + c_{kj})(a_1 + a_j)) \\ &= (((s-1)_{2j} + a_k)(a_j + c_{2k}) + c_{kj})(a_2 + a_j) \\ &= s_{2j}. \end{aligned}$$

Since h^2 is the identity, $h(s_{2j}) = s_{1j}$.

Now suppose $v_1 = 1$, $v_2 = -s$ and $v_k = 0$ for $k > 2$. Then, for $j > 2$,

$$\begin{aligned} h(c(v)) = h(s_{12}) &= h((s_{1j} + c_{j2})(a_1 + a_2)) \\ &= (s_{2j} + c_{j1})(a_1 + a_2) = s_{21} = c(Cv). \end{aligned}$$

Note that $(Cv)^{(i)} = C(v^{(i)})$ if $i > 2$ and $(Cv)^{(1)} = C(v^{(2)})$. With the aid of this it is easy to complete the proof. □

Lemma 3.9. *The endomorphisms f, g, h given above are in fact automorphisms of* $\mathrm{FM}(P(n,p))$.

PROOF. Recall $A = E_{(3)-r(4)}$. $A^{-1} = E_{(3)+r(4)}$ has the same form. Thus there is an endomorphism f' such that $f'(c(v)) = c(A^{-1}v)$. It follows that $ff'(a_i) = f'f(a_i) = a_i$ and $ff'(c_{1j}) = f'f(c_{1j}) = c_{1j}$. Thus f' is the inverse of f. Similarly g and h are automorphisms. □

THEOREM 3.10. *Let $A \in \mathrm{GL}(n,p)$. Then there is an automorphism f of $\mathrm{FM}(P(n,p))$ such that $f(c(v)) = c(Av)$ for all $v \in V$.*

PROOF. Let $A = A_1 \cdots A_k$ where each A_i is an elementary matrix of the form described in Lemma 3.4. For each i there is an automorphism f_i of $\mathrm{FM}(P(n,p))$ such that $f_i(c(v)) = c(A_i v)$. Let $f = f_1 \cdots f_k$. It is easy to see that $f(c(v)) = c(Av)$. □

LEMMA 3.11. *Let U be a subspace of V and let $u_1, \ldots, u_k$ be a basis of U. If $u \in U$, then $c(u) < c(u_1) + \cdots + c(u_k)$.*

PROOF. Choose $A \in \mathrm{GL}(n,p)$ such that $Ae_i = u_i$ where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. Let $w = A^{-1}u$; then $w \in \langle e_1, \ldots, e_k \rangle$. It follows easily from the definition of $c(w)$ that

$$c(w) < a_1 + \cdots + a_k = c(e_1) + \cdots + c(e_k).$$

Let f be the automorphism of $\mathrm{FM}(P(n,p))$ associated with A. Then

$$\begin{aligned} c(u) = c(Aw) &= f(c(w)) < f(c(e_1)) + \cdots + f(c(e_k)) \\ &= c(Ae_1) + \cdots + c(Ae_k) = c(u_1) + \cdots + c(u_k). \quad \Box \end{aligned}$$

If U is a subspace of V with basis $u_1, \ldots, u_k$, we now define $c(U) = c(u_1) + \cdots + c(u_k)$. Thus c maps $L(V)$ into $\mathrm{FM}(P(n,p))$ and by Lemma 3.11 the definition of $c(U)$ is independent of the choice of basis of U.

LEMMA 3.12. *c is a lattice homomorphism.*

PROOF. Let U, W be subspaces of V and choose $v_1, \ldots, v_k$ a basis of $U \cap W$, $v_1, \ldots, v_k, u_1, \ldots, u_r$ a basis of U, and $v_1, \ldots, v_k, w_1, \ldots, w_s$ a basis of W. Then $c(U) + c(W) = c(U + W)$ follows immediately from the definition.

Suppose $x_1, \ldots, x_t$ are independent vectors in V. Then there is an $A \in \mathrm{GL}(n,p)$ such that $Ae_i = x_i$, $i = 1, \ldots, t$. Since $\{c(e_1), \ldots, c(e_t)\} = \{a_1, \ldots, a_t\}$ is an independent set in $\mathrm{FM}(P(n,p))$ and since there is an automorphism of $\mathrm{FM}(P(n,p))$ corresponding to A, $c(x_1), \ldots, c(x_k)$ are independent in $\mathrm{FM}(P(n,p))$. Thus $\{c(v_1), \ldots, c(v_k), c(u_1), \ldots, c(u_r), c(w_1), \ldots, c(w_s)\}$ is independent. Hence

$$\begin{aligned} c(U)c(W) &= [c(v_1) + \cdots + c(v_k) + c(u_1) + \cdots + c(u_r)] \\ &\qquad \times [c(v_1) + \cdots + c(v_k) + c(w_1) + \cdots + c(w_s)] \\ &= c(v_1) + \cdots + c(v_k) = c(U \cap W). \quad \Box \end{aligned}$$

It is now easy to complete the proof of Theorem 3.2. The homomorphism $c\colon L(V) \to \mathrm{FM}(P(n,p))$ is onto since the generators of $\mathrm{FM}(P(n,p))$ are in its image. It is one-to-one since $L(V)$ is a simple lattice. Alternately c splits the natural map from $\mathrm{FM}(P(n,p))$ onto $L(V)$. □

We close with two corollaries. First it is shown in [8] that each of the lattices $L(\mathbf{Z}_p^n)$ is 4-generated. Thus $L(\mathbf{Z}_p^n)$ is a sublattice of FM(4). Since every finite planar modular lattice can be embedded into $L(\mathbf{Z}_p^n)$ for large enough n and p, we have the following corollary which improves the results of [3].

COROLLARY 3.13. *Every finite planar modular lattice can be embedded into* FM(4). □

Splitting modular lattices are defined in the introduction. We leave the proof of the next corollary to the reader.

COROLLARY 3.14. *For* $4 \leqslant n < \omega$ *and* p *a prime*, $L(\mathbf{Z}_p^n)$ *is a splitting modular lattice.* □

REFERENCES

1. P. Crawley and R. P. Dilworth, *Algebraic theory of lattices*, Prentice-Hall, Englewood Cliffs, N. J., 1973.

2. A. Day, *Splitting algebras and a weak notion of projectivity*, Algebra Universalis **5** (1975), 153–162.

3. R. Freese, *Planar sublattices of* FM(4), Algebra Universalis **6** (1976), 69–72.

4. ______, *The variety of modular lattices is not generated by its finite members*, Trans. Amer. Math. Soc. (to appear).

5. R. Freese and B. Jónsson, *Congruence modularity implies the Arguesian identity*, Algebra Universalis **6** (1976), 225–228.

6. M. Hall and R. P. Dilworth, *The imbedding problem for modular lattices*, Ann. of Math. **45** (1944), 450–456.

7. I. Halperin, Appendix to [**14**].

8. C. Herrmann, *On the equational theory of submodule lattices*, Proc. Univ. Houston Lattice Theory Conference, (Houston, Tex., 1973), Dept. of Math., Univ. Houston, Houston, Tex., 1973, pp. 105–118.

9. C. Herrmann and A. Huhn, *Lattices of normal subgroups which are generated by frames*, Lattice Theory, Colloq. Math. Soc. János Bolyai, vol. 14, North-Holland, Amsterdam, 1976, pp. 97–136.

10. A. Huhn, *Schwach distributive Verbände*. I, Acta Sci. Math. (Szeged) **33** (1972), 297–305.

11. ______, *On G. Grätzer's problem concerning automorphisms of a finitely presented lattice*, Algebra Universalis **5** (1975), 65–71.

12. F. Maeda, *Kontinuierlishe Geometrien*, Springer-Verlag, Berlin, 1958.

13. R. McKenzie, *Equational bases and non-modular lattice varieties*, Trans. Amer. Math. Soc. **174** (1972), 1–43.

14. J. von Neumann, *Continuous geometry*, Princeton University Press, Princeton, N. J., 1960.

15. R. Wille, *Aktuelle Probleme der Verbandstheorie*, preprint.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HAWAII 96822