McMaster University
DigitalCommons@McMaster

Open Access Dissertations and Theses | Open Dissertations and Theses

3-1985

Varieties of Modular Ortholattices

Michael Stewart Roddy

Follow this and additional works at: http://digitalcommons.mcmaster.ca/opendissertations

Part of the Mathematics Commons

Recommended Citation
Roddy, Michael Stewart, "Varieties of Modular Ortholattices" (1985). *Open Access Dissertations and Theses.* Paper 1301.

This Thesis is brought to you for free and open access by the Open Dissertations and Theses at DigitalCommons@McMaster. It has been accepted for inclusion in Open Access Dissertations and Theses by an authorized administrator of DigitalCommons@McMaster. For more information, please contact scom@mcmaster.ca.

VARIETIES OF MODULAR ORTHOLATTICES

By

MICHAEL S. RODDY, M.Sc.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements

for the Degree

Doctor of Philosophy

McMaster University

© March 1985

VARIETIES OF MODULAR ORTHOLATTICES

DOCTOR OF PHILOSOPHY
(Mathematics)

McMASTER UNIVERSITY
Hamilton, Ontario

TITLE: Varieties of Modular Ortholattices

AUTHOR: Michael Stewart Roddy, B.Sc. (Lakehead University)
M.Sc. (McMaster University)

SUPERVISOR: Dr. G. Bruns

NUMBER OF PAGES: v, 42

ABSTRACT

This thesis describes the bottom of the lattice of varieties of modular ortholattices. The theorem that is proved is

Theorem. Every variety of modular ortholattices which is different from all the $[MO_n]$, $0 \le n \le \omega$, contains $[MO_\omega]$.

This theorem is proved by translating the problem, at least partially, into the language of regular rings.

ACKNOWLEDGEMENTS

I wish to thank Professors B. Banaschewski and B. Mueller, Professor A. Day and most of all my supervisor Professor G. Bruns. For financial support I am indebted to N.S.E.R.C., the Ontario government and McMaster University. I would also like to thank Phil Smedley for many interesting and helpful discussions. Finally, my thanks go to Cheryl McGill and Carolyn Aho for typing this thesis.

TABLE OF CONTENTS

		Page
	INTRODUCTION	1
1.	PRELIMINARIES (MOL'S)	2
2.	REGULAR RINGS	6
3.	OC'S AND INVOLUTIONS	11
4.	TECHNICALITIES I	17
5.	TECHNICALITIES II	23
6.	TECHNICALITIES III	29
7.	RESULTS	36
8.	CONCLUDING REMARKS	41
	BIBLIOGRAPHY	42

Introduction.

In this thesis the bottom of the lattice of varieties of modular ortholattices (bounded modular lattices equipped with an orthocomplementation) is described. Avoiding the language of modular ortholattices as much as possible the main result may be stated as

Theorem. The lattice of varieties of modular ortholattices contains a countably infinite ascending chain with least element the trivial variety and with supremum the variety [MOω]. Every variety of MOL's not in this chain contains [MOω].

The material in [3] reduces the problem to showing that certain subdirectly irreducible algebras must contain a nontrivial Boolean interval. The problem is then translated into a ring-theoretic setting and the theorem depends on the proof of a technical lemma concerning certain lattices of submodules. This lemma is stated at the end of section 1.

The proof of the lemma constitutes the bulk of this thesis. The reduction from the general case to the setting of the lemma is not given until section 7. It is therefore suggested that the reader scans section 7 before commencing section 3 in order to aid motivation.

Claims stated without proof or specific reference are either well known, eg. (1.1), or very easy to prove, eg. (7.1). In one instance proofs are nested, see (4.1). This has been done because these claims would be difficult to formulate outside the context of (4.1). The symbol $\square$ signifies the end of a proof.

1. Preliminaries (MOL's).

A lattice L is modular in case $a \vee ((a \vee b) \wedge c) = (a \vee b) \wedge (a \vee c)$ for all $a,b,c \in L$. A bounded modular lattice, with least element 0 and greatest element 1, is complemented in case for each $x \in L$ there exists $y \in L$ with $x \vee y = 1$ and $x \wedge y = 0$. Complemented modular lattices are discussed in [4]. If L is complemented modular then the set of elements in L with unique complements is called the center of L, written C(L).

(1.1) The map $L \to [o,a] \times [o,a']$ given by $x \rightsquigarrow (x \wedge a,\ x \wedge a')$, where a' is a complement of a, is an isomorphism if and only if $a \in C(L)$. If the map is an isomorphism then its inverse is given by $(s,t) \rightsquigarrow s \vee t$.

It follows that

(1.2) L is irreducible if and only if $C(L) = \{0,1\}$.

(1.3) (15.4, page 147, [4]) C(L) is a sublattice of L and as a sublattice is Boolean.

An antiautomorphism of a lattice is a lattice isomorphism f between a lattice L and its dual, i.e. a bijection with $f(x \vee y) = f(x) \wedge f(y)$ and $f(x \wedge y) = f(x) \vee f(y)$ for all $x,y \in L$. An antiautomorphism f is of period two in case $f(f(x)) = x$ for all $x \in L$, and is a complementation if $x \vee f(x) = 1$ and $x \wedge f(x) = 0$ for all $x \in L$. An antiautomorphism $x \rightsquigarrow x'$ which is of period two and is a complementation is called an orthocomplementation (abbreviated: OC). A modular ortholattice (abbreviated: MOL) is an algebra $L = (|L|;\vee,\wedge,',0,1)$ where $(|L|;\vee,\wedge,0,1)$ is a bounded modular lattice and ' is an OC. In an MOL L, $x,y \in L$ are

said to commute, written xCy, if and only if $x = (x \wedge y) \vee (x \wedge y')$.

(1.4) In an MOL L

(1) xCy implies yCx

(2) For $X \subseteq L$ let $C(X) = \{a \in L: aCx \text{ for all } x \in X\}$.

Then $C(X)$ is a subalgebra of L.

(3) L is Boolean if and only if $L = C(L)$.

Observe that $C(L)$ defined in (1.4.b) coincides with $C(L)$ as defined previously because (1.1) gives that $a \in C(L)$ if and only if $(x \wedge a) \vee (x \wedge a') = x$ for all $x \in L$. If $a,b \in L$ with $a \leq b$ then $[a,b]$ inherits an OC given by $x \overset{\#}{\rightsquigarrow} (a \vee x') \wedge b$. In fact

(1.5) $([a,b];\vee,\wedge,\#,a,b) \in HS(L)$.

The above theory is developed in the more general setting of orthomodular lattices in [11].

The simplest examples of MOL's are the MOn's. Let n be a cardinal number greater than 1, MOn consists of $2n$ pairwise incomparable points and the bounds. Define MO0 to be the one element MOL and MO1 to be the two element Boolean algebra. Let [MOn] be the variety of MOL's generated by MOn, $0 \leq n \leq \omega$. It follows from Jónsson [10] that [MO(n+1)] covers [MOn], $0 \leq n < \omega$, in the lattice of varieties of MOL's. Every MOL with more than one element has distinct bounds and hence every variety of MOL's which is not contained in [MO0] contains [MO1]. That every variety of MOL's which is not contained in [MO1] contains [MO2] follows from

(1.6) If L is a nonBoolean MOL then there exists $0 \neq \gamma \in L$ so that MO2 is a subalgebra of the MOL $[0,\gamma]$.

The main (explicit) result of [3] is

(1.7) (page 1, [3]) Every variety of MOL's which is not contained in [MO2] contains [MO3].

The main result of this thesis is the stronger

Theorem. Every variety of MOL's which is different from all the [MOn], $0 \le n \le \omega$, contains [MOω].

This theorem is a weakening of a conjecture made by G. Bruns. A projective plane is an irreducible complemented modular lattice of height 3.

Conjecture. (page 1, [3]) Every variety of MOL's which is different from all the [MOn], $0 \le n \le \omega$, contains a projective plane (as the lattice reduct of an algebra).

That the conjecture is stronger than the theorem follows from the important theorem of Baer.

(1.8) ([2]) Every projective plane which admits an OC (a polarity without an absolute point) is infinite.

The algebra MOω can be constructed as an ultraproduct of the MOn, $0 \le n < \omega$, and so

(1.9) Every variety of MOL's which contains infinitely many of the [MOn], $0 \le n \le \omega$, contains [MOω].

An n frame, $n \ge 2$, (see [5]) in a bounded modular lattice L is an (n+1)-tuple $x_1,\ldots,x_{n+1}$ such that

$$(1) \quad \bigvee_{i \ne j} x_i = 1, \quad j=1,\ldots,n+1$$

$$(2) \quad x_i \wedge \bigvee_{i \ne j \ne k \ne i} x_k = 0, \quad 1 \le i,j \le n+1$$

A familiar example of a 3-frame is four points in general position in a projective plane. If R is a ring then $<(1,0,0,\ldots,0)>_R$, $<(0,1,0,\ldots,0)>_R$, ..., $<(0,0,\ldots,0,1)>_R$, $<(1,1,\ldots,1)>_R$, where $<(a_1,\ldots,a_n)>_R$ is the right submodule of R^n generated by $(a_1,\ldots,a_n) \in R^n$, is an n-frame in the lattice of right submodules of R^n. It is called the canonical frame.

If L is an MOL then an n-frame in L is called orthogonal in case $x_i C x_j$, $1 \le i,j \le n$. For example if $R = \mathbb{R}$ and the OC is the one induced by the usual inner product then the canonical n-frame is orthogonal.

The main body of this thesis, sections 4, 5 and 6, is devoted to proving the somewhat technical.

<u>Lemma</u>. Let $L = \bar{L}(R^3)$ be an MOL with orthogonal canonical 3-frame for some ring R with prime characteristic. Then $MO_\omega \in HSP(L)$ or L contains a nontrivial Boolean interval of the form $[0,x]$.

Sections 2 and 3 are introductory. Section 7 uses results from [3], a method suggested by A. Day [6], and the above lemma to prove the main theorem.

Finally some remarks on notation. An MOL L may admit several different OC's only one of which is the operation of the algebra. We adopt the convention that, unless otherwise stated, the OC associated with L as an MOL is written '. Also, subscripts on an interval indicate which algebra this interval is to be taken in. Such subscripts are only used when necessary in order to avoid confusion.

2. Regular Rings.

In this section some of the theory of regular rings ([8], [13] and [14]) is recalled and a few observations are made. Much of this and the following section is taken from the first four chapters of section II of [13]. All rings considered have unit.

Let R be a ring and $n \in \mathbb{N}$. $L(R^n)$ will be the modular lattice of right submodules of R^n, $\bar{L}(R^n)$ will be the poset of finitely generated right submodules of R^n. The right submodule of R^n generated by a set X will be written $\langle X\rangle_R$, if no confusion seems likely then the subscript R will be dropped. The principal right ideal generated by $a \in R$ will be written aR. On the rare occassion that left submodules are considered subscripts will always be included, i.e. $L({}_RR^n)$, $\bar{L}({}_RR^n)$, ${}_R\langle X\rangle$ and Ra are the lattice of left submodules of R^n, the poset of finitely generated left submodules of R^n, the left submodule of R^n generated by the set X and the principal left ideal generated by $a \in R$ respectively. An element $e \in R$ is idempotent in case $e = e^2$.

(2.1) (Corollary, page 69, [13]) Let R be a ring. Then

(1) e is an idempotent if and only if 1-e is an idempotent.

(2) $eR = \{a \in R: ea = a\}$

(3) eR and (1-e)R are complements in L(R)

(4) If eR = fR and (1-e)R = (1-f)R where e and f are idempotents then e=f.

(2.2) (Theorem 21.1, page 69, [13]) Two right ideals I and J are complements in L(R) if and only if there exists an idempotent $e \in R$

with $eR = I$ and $(1-e)R = J$. This property characterizes uniquely the idempotent e.

(2.3) (Theorem 2.2, page 70, [13]) T.A.E.

(1) Every principal right ideal has a complement in $L(R)$.

(2) For every $a \in R$ there exists an idempotent $e \in R$ with $aR = eR$.

(3) For every $a \in R$ there exists $r \in R$ with $ara = a$.

(4) For every $a \in R$ there exists an idempotent $f \in R$ with $Ra = Rf$.

(5) Every principal left ideal has a complement in $L({}_RR)$.

A ring is said to be regular in case it possesses one of the above equivalent properties. Henceforth R will be a regular ring.

For each right ideal I of R we define $\ell\mathrm{Ann}(I) = \{y \in R: yz = 0, \text{ for all } z \in I\}$ and for each left ideal J of R we define $r\mathrm{Ann}(J) = \{y \in R: zy = 0, \text{ for all } z \in J\}$.

(2.4) (Corollary 1, corollary 2, page 71, [13]) The mapping $I \rightsquigarrow \ell\mathrm{Ann}(I)$ is an anti-isomorphism (an order reversing bijection) between the posets $\bar{L}(R)$ and $\bar{L}({}_RR)$. The inverse of this map is given by $J \rightsquigarrow r\mathrm{Ann}(J)$.

(2.5) (Theorem 2.3, page 71, [13]) The join (in $L(R)$) of two principal right ideals is again a principal right ideal.

(2.6) (Theorem 2.4, page 72, [13]) $\bar{L}(R)$ is a complemented modular lattice, in fact a sublattice of $L(R)$.

For any ring S and $A \subseteq S$ we define $Co(A) = \{s \in S: \ as = sa$, for all $a \in A\}$. In particular the center of S is Co(S).

(2.7) Co(A) is a subring of S.

(2.8) (theorem 2.5, page 74, [13]) Co(R) is regular.

(2.9) (lemma 2.9, page 76, [13]) A principal right ideal I of R is uniquely represented as I = eR, e an idempotent, if and only if $e \in Co(R)$.

(2.10) The map $aCo(R) \rightsquigarrow aR$ is a lattice isomorphism $\bar{L}(Co(R)) \rightarrow C(\bar{L}(R))$.

<u>Proof</u>. Clearly this map is well defined and order preserving. Let $a \in Co(R)$. Since Co(R) is regular there exists e, $r \in Co(R)$ with e idempotent so that $eCo(R) = aCo(R)$ and $ar = e$. But $a \in eCo(R)$ if and only if $ea = a$ if and only if $a \in eR$. It follows that $eR = aR$. If a, $b \in Co(R)$ with $aR \subseteq bR$ then there exists idempotents e, $f \in Co(R)$ so that $eR = aR \subseteq bR = fR$. But $eR \subseteq fR$ if and only if $fe = e$ if and only if $eCo(R) \subseteq fCo(R)$. Hence, the map is an order embedding. That this map is onto $C(\bar{L}(R))$ follows immediately from (2.9). An order embedding onto a lattice is a lattice embedding. □

Maps similar to the one defined above will be used throughout the remainder of this work. If S is a subset of R which, with the restricted operations except possibly the unit, forms a ring then the map $aS \rightsquigarrow aR$, $a \in S$, is well defined and monotone. When this map is a lattice embedding (not necessarily preserving bounds) then we write $\bar{L}(S) \overset{i}{\hookrightarrow} L(R)$ and we call i the canonical injection.

For an idempotent $e \in R$ let $R(e) = \{a \in R: \ eae = a\}$.

(2.11) (Theorem 2.11, page 77, [13]) $R(e)$ is a regular ring with e as unit.

(2.12) $\bar{L}(R(e)) \xrightarrow{i} \bar{L}(R)$ onto $[o,eR]_{\bar{L}(R)}$.

Proof. Clearly the map is well defined and monotone. If $fR \subseteq eR$, f an idempotent, then $feR = fR$ since $fef = f^2 = f$. Also $e(fe)e = efe = fe$. This establishes that the map is onto $[o,eR]_{\bar{L}(R)}$. If $aR \subseteq bR$, $a, b \in R(e)$, then there exists $r \in R$ with $br = a$. But $bere = bre = ae = a$, so $aR(e) \subseteq bR(e)$. It follows that the map is an order embedding onto a sublattice of $\bar{L}(R)$ and therefore a lattice embedding. □

For a ring S and $n \in \mathbb{N}$ let S_n be the ring of $n \times n$ matrices over S.

(2.13) (Theorem 2.14, page 81, [13]) S_n is regular if and only if S is regular.

The next theorem is proved in [13] (see pages 80, 81 and appendix 3, page 90) but it is not explicity stated. It is stated and proved in Skornyakov [14], this source is cited. Let S be a ring and $n \in N$, define $L(S^n) \xrightarrow{\phi} L(S_n)$ by $M \to \{(a_{ij}): (a_{1j}, a_{2j}, \ldots, a_{nj}) \in M\}$ and $L(S_n) \xrightarrow{\psi} L(S^n)$ by $I \to \{(a_1, \ldots, a_n): (a_1, \ldots, a_n)$ is the column of a matrix in $I\}$.

(2.14) (Proposition 14, page 13, [14]) ϕ and ψ are inverse lattice isomorphisms. Furthermore finitely generated right submodules and finitely generated right ideals correspond to each other.

(2.15) (Corollary) $\bar{L}(R^n) \xrightarrow{\phi} \bar{L}(R_n)$, $n \in N$, is an isomorphism and finitely generated right submodules of R^n are at most n generated.

A homogeneous basis of order n, $n \geq 2$, in a bounded modular lattice L is an n-tuple $(x_1,\ldots,x_n)$ such that

(1) $\bigvee x_i = 1$

(2) $x_i \wedge \bigvee_{i \neq j} x_j = 0$, $i=1,\ldots,n$.

(3) For each i,j there exists y so that $x_i \vee y = x_j \vee y = 1$ and $x_i \wedge y = x_j \wedge y = 0$.

(2.16) If $(x_1,\ldots,x_{n+1})$ is an n-frame then $(x_1,\ldots,x_n)$ is a homogeneous basis of order n.

<u>Proof.</u> (1) and (2) are immediate. For (3) let $y = \bigvee_{j \neq k \neq i} x_k$. □

R is said to be of order n in case $\bar{L}(R)$ has a homogeneous basis of order n (see pages 93, 100, [13]).

(2.17) (Theorem 4.1, page 104, [13]) If R is of order $n \geq 2$ then the only ring automorphism $R \xrightarrow{\phi} R$ such that $\phi(a)R = aR$ for all $a \in R$, is the identity.

3. OC's and Involutions.

In this section the relationship between OC's on $\bar{L}(R)$, R a regular ring, and involutions on R is described. An additive bijection $f: R \longrightarrow R$ such that $f(ab) = f(b)f(a)$, for all $a,b \in R$, is called an antiautomorphism of R.

(3.1) (1) (theorem 4.3, page 113, [13]) If f is an antiautomorphism of R then $aR \mapsto rAnnf((a))$ is an antiautomorphism of $\bar{L}(R)$. The map f is said to generate F. If R is of order $n \geq 3$ then each antiautomorphism of $\bar{L}(R)$ is generated by a unique antiautomorphism of R.

(2) (Lemma 4.3, page 114, [13]) If F is generated by f then $F(F(aR)) = f(f(a))R$ for all $a \in R$.

(3) (see theorem 4.4, page 114, [13]) If f is of period two, ie. $f(f(a)) = a$ for all $a \in R$, then F is of period two. Conversely, if F is of period two, generated by f and if R is of order $n \geq 2$ then f is of period two.

(4) (Theorem 4.5, page 114, [13]) If f is an antiautomorphism of R of period two and f generates F then T.A.E.

(a) $I \wedge F(I) = 0$, for all $I \in \bar{L}(R)$

(b) $I \vee F(I) = 1$, for all $I \in \bar{L}(R)$

(c) For every $a \in R$ there exists $z \in R$ with $zf(a)a = a$

(d) $f(a)a = 0$ implies $a = 0$

(e) For every $a \in R$ there exists a (unique) idempotent $e \in R$ with $e = f(e)$ and $aR = eR$.

Proof of (3.1.3). If f is of period two then (2) implies that F is of period two. If F is of period two and f generates F then $aR = f(f(a))R$ for all $a \in R$. Since R is of order $n \geq 2$ (2.17) applies and f^2 is the identity on R. □

An antiautomorphism $a \to a^*$ of R of period two such that $a^*a = 0$ implies $a = 0$ is called an involution on R. If * is an involution on R then R is called *regular, $a \in R$ with $a = a^*$ is called *self-adjoint and a *self-adjoint idempotent is called a *projection. The set of *projections of R is written *Pr(R). The relevant parts of (3.1) may now be stated in terms of involutions and OC's.

(3.2) (1) If R is *regular then $aR \rightsquigarrow r\mathrm{Ann}(Ra^*)$ is an OC, ', on $\bar{L}(R)$. The involution * is said to generate the OC '. If R is of order $n \geq 3$ then each OC on $\bar{L}(R)$ is generated by a unique involution on R.

(2) If $e \in {}^*Pr(R)$ then $(eR)' = (1 - e)R$.

Proof of (3.2.2). Since $e + 1 - e = 1$, $eR \vee (1 - e)R = 1$. Since $e^*(1 - e) = e(1 - e) = 0$, $(1 - e)R \leq (eR)'$. □

If $n \geq 4$ and $\bar{L}(R^n)$ has an orthogonal n-frame then F. Maeda [12] has shown that corresponding to the OC on $\bar{L}(R^n)$ is a "Hermitian form". He only uses the fact that $n \geq 4$ to invoke the coordinatization theorem of von Neumann [13], the remainder of the proof works perfectly well for the case $n = 3$.

(3.3) ([12]) If $\bar{L}(R^3)$ is an MOL with orthogonal canonical 3-frame then there exists an involution * on R and invertible *self-adjoint elements $\alpha, \beta \in R$ so that for $M \in L(R^3)$

$M' = \{(a,b,c): a^*m_1 + b^*\alpha m_2 + c^*\beta m_3 = 0$ for all $(m_1,m_2,m_3) \in M\}$.

The triple $(\alpha,\beta,*)$ is called a form associated with $'$.

If $e \in {}^*Pr(R)$ then by combining (2.12) and (2.14) we know that $\mathcal{L}(R(e)^3) \xrightarrow{\phi} \mathcal{L}(R(e)_3) \overset{i}{\hookrightarrow} \mathcal{L}(R_3) \xrightarrow{\psi} \mathcal{L}(R^3)$ is onto $[0,a(e)]_{\mathcal{L}(R^3)}$, where $a(e) = \langle(e,0,0), (0,e,0), (0,0,e)\rangle_R$, and a lattice injection. Call the composite isomorphism $\mathcal{L}(R(e)^3) \xrightarrow{\kappa} [0,a(e)]_{\mathcal{L}(R^3)}$. Then $\mathcal{L}(R(e)^3)$ inherits an OC given by $M \rightsquigarrow \kappa^{-1}((\kappa(m))')$, which we will also call $'$.

(3.4)' A form associated with $'$ on $\mathcal{L}(R(e)^3)$ is $(e\alpha e, e\beta e, *)$.

<u>Proof</u>. Since $e \in {}^*Pr(R)$, $*|R(e)$ is an involution on $R(e)$. The map κ is given by the composition

$\mathcal{L}(R(e)^3) \xrightarrow{\phi} \mathcal{L}(R(e)_3) \overset{i}{\hookrightarrow} \mathcal{L}(R_3) \xrightarrow{\psi} \mathcal{L}(R^3)$ which is an embedding onto $[0,a(e)]_{\mathcal{L}(R^3)}$. Let $M \in \mathcal{L}(R(e)^3)$. There exists $(e_{ij}) \in R(e)_3$ so that $M = \langle(e_{1j},e_{2j},e_{3j}): j = 1,2,3\rangle_{R(e)}$ and $\phi(M) = (e_{ij})R(e)_3$. Hence $i(M) = (e_{ij})R_3$ and $\kappa(M) = \{(a_1,a_2,a_3): (a_1,a_2,a_3)$ is the column of a matrix in $(e_{ij})R_3\} = \langle(e_{1j},e_{2j},e_{3j}): j = 1,2,3\rangle_R = \langle M\rangle_R$. Therefore for $a,b,c \in R(e)^3$ we have the following equivalences

$(a,b,c) \in M'$

if and only if

$\langle(a,b,c)\rangle_{R(e)} \le \kappa^{-1}((\kappa(M))')$

if and only if

$\kappa(\langle(a,b,c)\rangle_{R(e)}) \le (\kappa(M))'$

if and only if

$\langle(a,b,c)\rangle_R \le (\langle M\rangle_R)'$

if and only if

$a^*n_1 + b^*\alpha n_2 + c^*\beta n_3 = 0$, for all $(n_1,n_2,n_3) \in \langle M\rangle_R$

if and only if

$a^*e_{1j} + b^*\alpha e_{2j} + c^*\beta e_{3j} = 0$, $j=1,2,3$

if and only if

$a^*e_{1j} + b^*e\alpha e\ e_{2j} + c^*e\beta e\ e_{3j} = 0$, $j=1,2,3$

if and only if

$a^*m_1 + b^*e\alpha e\ m_2 + c^*\ e\beta e\ m_3 = 0$, for all $(m_1,m_2,m_3) \in M$. □

If $a \in R$ is *self-adjoint and $e \in {}^*Pr(R)$ with $aR = eR$ then, since $ea = a = a^* = a^*e = ae$, $a \in R(e)$. And, since there exists $b \in R$ with $e = ab = b^*a^* = b^*a$, we know that a is invertible in the ring $R(e)$. The symbol a^{-1} is used for this "local inverse" of a. We modify earlier notation and will write $C(a)$ for $C(\{a\})$ and b Co a for $b \in Co(a)$.

(3.5) (1) $a^{-1} = a^{*-1}$

(2) For $b \in R$, a Co b if and only if a^{-1}Co b.

<u>Proof</u>. <u>Re</u>(1). If $e = ab$ then let $a^{-1} = eb$. First of all, $a^{-1} \in R(e)$ so $a^{-1*} \in R(e)$. Now a^{-1} is a right inverse of a in $R(e)$ and a^{-1*} is a left inverse of a in $R(e)$. It follows that $a^{-1} = a^{-1*}$.

<u>Re</u>(2). If $ab = ba$ then $a^{-1}b = a\ a^{-2}b = a^{-2}ba = a^{-2}ba^2a^{-1} = a^{-2}a^2\ ba^{-1} = aa^{-1}ba^{-1} = a^{-1}ba^2a^{-2} = a^2a^{-1}ba^{-2} = aba^{-2} = ba^{-1}$. □

(3.6) Let R be *regular and $Z \subseteq R$ a subring of R with $*|_Z = id_Z$. There exists a regular subring S of R with $*|_S = id_S$ and $Z \subseteq S$.

Proof. Let $\mathcal{S}$ be the set of all subrings S of R with

(1) $Z \subseteq S$

and

(2) $*|_S = id_S$.

Clearly $\mathcal{S}$ is inductive. By Zorn's lemma there exists a maximal $S \in \mathcal{S}$. If $a \in S$ then $S \cup \{a^{-1}\}$ generates a ring which satisfies (1). But $*|_S = id_S$ implies that S is commutative. This with (3.5.2) implies that the ring generated by $S \cup \{a^{-1}\}$ is commutative. Every element in this ring may be expressed as a polynomial in a^{-1} with coefficients in S. All such polynomials are *self-adjoint, and (2) is satisfied. It follows that $a^{-1} \in S$. This is true for any $a \in S$ and therefore S is regular. □

(3.7) Let R be *regular, $F \subseteq R$ a subring of R which is a field with $*|_F = id_F$. Also let $\{a_1,\ldots,a_n\} \subseteq R$ with each $a_i \in Co(F \cup \{a_1,\ldots,a_n\})$ and so that for each i there exists $k_i > 1$ with $a_i^{k_i} = a_i$. Then there exists $e_1,\ldots,e_m \in (*Pr(R)\setminus\{0\}) \cap Co(F \cup \{a_1,\ldots,a_n\})$ so that

(1) $\sum_{i=1}^{m} e_i = 1,\ e_i e_j = \delta_{ij}\, e_j$

and

(2) $\{ze_i:\ z \in Co(F \cup \{a_1,\ldots,a_n\})\}$ generates a field F_i in $R(e_i)$ with $*|F_i = id_{F_i}$. Furthermore, if F is finite then so is each F_i.

Proof. Let S be the subring of R generated by $F \cup \{a_1,\ldots,a_n\}$. Since S is generated by commuting *self-adjoint elements, $*|_S = id_S$. S may be considered as an F-vector space and as such is spanned by the set $\{a_1^{\ell_1} a_2^{\ell_2} \ldots a_n^{\ell_n}:\ 0 \le \ell_i \le k_i\}$. It follows that S is finite

dimensional over F. Every ideal of S is an F vector subspace of S and it follows that the lattice of ideals of S is of finite height. Hence S is a semisimple ring (see page 153, [1]). The Wedderburn-Artin theorem (page 154, [1]) guarantees that S is a ring-direct sum of matrix rings over division rings. The fact that S is commutative implies that each of these matrix rings is in fact a field. If F is finite then so is S. □

If $a = a^*$ and $a^m = 0$ then for k with $m \leq 2^k$ we have $a^{2^k} = 0$. But $0 = a^{2^k} = (a^{2^{k-1}})^*(a^{2^{k-1}})$ implies $a^{2^{k-1}} = 0$. It follows by induction that $a = 0$. Hence

(3.8) If $a = a^*$ and $a^m = 0$ then $a = 0$.

4. Technicalities I.

Let $L = \bar{L}(R^3)$ be an MOL with orthogonal canonical frame and associated form $(\alpha,\beta,*)$. Assume that $MO\omega \notin HSP(L)$ and that R has prime characteristic. In this section we take the first steps toward proving the lemma given in section 1.

(4.1) Let $0 \neq a = a^* \in R$. There exists $m > 0$ with $a^{m+1} = a$.

Proof. Let $0 \neq a = a^* \in R$, we will prove (4.1) via a long series of claims. Let $aa^{-1} = e$ and let Z be the subring of R generated by a. Since $*|_Z = id_Z$ we may apply (3.6) to obtain a regular subring S of R with $Z \subseteq S$ and $*|_S = id_S$. Since $*|_S = id|_S$, S is commutative and since $a, a^{-1} \in S$ we have $e \in *Pr(S)$. Our first claim depends only on the commutativity of S.

Claim 1. If $f, g \in *Pr(S)$ with $fg = g$ and $r \in S(f)$ then if rg is noninvertible in S(g) it follows that r is noninvertible in S(f).

Proof. If $rr^{-1} = f$ then $rgr^{-1}g = rr^{-1}g = fg = g$. □

Define two sequences, $(m_i)_{i=-1}^{\infty}$ of natural numbers and $(e_i)_{i=-1}^{\infty}$ of *projections recursively by:

Step -1 $e_{-1} = e$ and $m_{-1} = 0$.

Step (i+1) If $e_i \neq 0$ and there exists $m > 0$ with $(a^m - e)e_i$ noninvertible in $S(e_i)$ then let m_{i+1} be the least such m and let $e_{i+1} = (a^{m_{i+1}} - e)e_i\,[(a^{m_{i+1}} - e)e_i]^{-1} \in *Pr(S(e_i))$. If $e_i = 0$ or if no such m exists then let $e_{i+1} = e_i$ and $m_{i+1} = m_i$.

Claim 2. If $0 \leq n \leq m_i$ and $e_i \neq 0$ then $(a^n - e)e_i$ is invertible in $S(e_i)$, $0 \leq i$.

Proof. If $e_i \neq 0$ then since $e_{i-1}e_i = e_i$, $e_{i-1} \neq 0$. Assume that $(a^n - e)e_i$ is noninvertible in $S(e_i)$ for some $n > 0$. Then, by claim 1, $(a^n - e)e_{i-1}$ is noninvertible in $S(e_{i-1})$. Since $e_{i-1} \neq 0$ and since there exists $n > 0$ with $(a^n - e)e_{i-1}$ noninvertible in $S(e_{i-1})$ we know that m_{i+1} is the least m with $(a^m - e)e_{i-1}$ noninvertible in $S(e_{i-1})$. It follows that $m_i \leq n$, and since $(a^{m_i} - e)e_{i-1}\ [(a^{m_i} - e)e_{i-1}]^{-1} = e_i$ we have $m_i \neq n$. □

Claim 3. The sequence $(m_i)_{i=-1}^{\infty}$ is increasing.

Proof. If $m_{i+1} \neq m_i$ then $e_i \neq 0$ and $(a^{m_{i+1}} - e)e_i$ is noninvertible in $S(e_i)$. It follows from claim 2 that $m_i < m_{i+1}$. □

Claim 4. If $m_i = m_{i+1}$ then $e_i = 0$ or $(a^k - e)e_i$ is invertible in $S(e_i)$ for all $k > 0$.

Proof. If $e_i \neq 0$ and $(a^k - e)e_i$ is noninvertible in $S(e_i)$ for some $k > 0$ then first of all, by claim 2, $m_i < k$. Secondly m_{i+1} is the least such k. Therefore if $e_i \neq 0$ and $m_i = m_{i+1}$ no such k exists. □

By claim 3 either $(m_i)_{i=-1}^{\infty}$ is strictly increasing or there exists a least s with $m_s = m_{s+1}$. If there exists such an s then, by claim 5, either $e_s = 0$ or $e_s \neq 0$ and $(a^k - e)e_s$ is invertible in $S(e_s)$ for all $k > 0$. We will dispose of the case $e_s = 0$ first.

Claim 5. If $m_o = 0$ then $m_k = 0$ and $e_k = e$ for all $k \geq 0$.

Proof. If $m_o = 0$ then $e_o = e$ and $(a^m - e)e_o$ is invertible in $S(e_o)$ for all $m > 0$. If $m_i = 0$, $e_i = e$ and $(a^m - e)e_i$ is invertible in $S(e_i)$ for all $m > 0$ then (applying step (i+1)) we obtain $m_{i+1} = m_i$, $e_{i+1} = e_i$ and consequently $(a^m - e)e_{i+1}$ is invertible in $S(e_{i+1})$ for all $m > 0$. It follows by induction that $m_k = 0$ and $e_k = e$ for all $k \geq 0$. □

Claim 6. If $m_o \neq 0$ then $(a^{m_i} - e)e_{i-1}S = e_iS$.

Proof. If $m_o \neq 0$ then $e_o = (a^{m_o} - e)e\,[(a^{m_o} - e)e]^{-1}$. If m_{i+1} is the least m with $(a^m - e)e_i$ noninvertible in $S(e_i)$ then $e_{i+1} = (a^{m_{i+1}} - e)e_i\,[(a^{m+1} - e)e_i]^{-1}$. Otherwise $m_{i+1} = m_i$ and $e_{i+1} = e_i$. The result follows by induction. □

Claim 7. If $e_s = 0$ (and s is the least such number) then there exists $m > 0$ with $a^{m+1} = a$.

Proof. Let $m = \prod_{0 \le i \le s} m_i$. If $m = 0$ then by claim 3 $m_o = 0$ and it follows from claim 5 that $0 = e_s = e$. But if $e = 0$ then $a = 0$, a contradiction. Therefore, $m > 0$. For $0 \le i \le s$ let $f_i = (e_{i-1} - e_i) \in {}^*Pr(S(e))$. Since $(a^{m_i} - e)e_{i-1}S = e_iS$, see claim 6, we have $(a^{m_i} - e)e_{i-1} = (a^{m_i} - e)e_{i-1}e_i = (a^{m_i} - e)e_i$. Let $n_i = mm_i^{-1} \in \mathbb{N}$. Then $a^m f_i = (a^{m_i} f_i)^{n_i} = [a^{m_i}(e_{i-1} - e_i)]^{n_i} = [e_{i-1} - e_i]^{n_i} = f_i^{n_i} = f_i$. Also $\sum_{i=0}^{s} f_i = e - e_o + e_o - e_1 + \ldots + e_{s-1} = e$. Therefore $a^m = a^m e = a^m \sum_{i=0}^{s} f_i = \sum_{i=0}^{s} a^m f_i = \sum_{i=0}^{s} f_i = e$. □

In order to complete the proof of (4.1) we need the following

Proposition. Let $n \in \mathbb{N} \cup \{\omega\}$, $0 \neq f \in {}^*Pr(S(e))$ with $(a^k - e)f$ invertible in $S(f)$ for all $0 < k < n$. Then $MO[n] \in HSP(L)$ where $[n]$ is the number of odd numbers less than n.

Before setting out to prove this proposition observe how it handles the two remaining cases. If $(m_i)_{i=-1}^{\infty}$ is strictly increasing then the proposition may be applied with $n = m_i$ and $f = e_i$ to obtain $MO[m_i] \in HSP(L)$. It follows from (1.9) that $MO\omega \in HSP(L)$. If $e_s \neq 0$ and $(a^k - e)e_s$ is invertible in $S(e_s)$ for all $k > 0$ then the proposition may be applied with $n = \omega$ and $f = e_s$ to obtain $MO\omega \in HSP(L)$. Since $MO\omega \notin HSP(L)$ these two cases cannot occur. It remains to prove the

proposition.

Let $A = \{<(a^{-s}f, f, 0)>_R \in L(R^3)$: s is odd, $0 < s < n\}$ and let $A' = \{y = x' \wedge <(f, 0, 0), (0, f, 0)>_R : x \in A\}$.

<u>Claim 8</u>. $A' = \{<(-a^s f\alpha f, f, 0)>_R$: s is odd, $0 < s < n\}$.

<u>Proof</u>. Let $0 < s < n$ with s odd. Then $(a^{-s}f)^* (-a^s f\alpha f) + f^*\alpha f = -f a^{-s}a^s f\alpha f + f\alpha f = 0$ and $<(-a^s f\alpha f, f, 0)>_R \leq <(a^{-s}f, f, 0)>'_R$. Let $(b_o, c_o, d) \in <(a^{-s}f, f, 0)>'_R \wedge <(f, 0, 0), (0, f, 0)>_R$. Since $(b_o, c_o, d) \in <(f, 0, 0), (0, f, 0)>'_R$ we know that $d = 0$ and by (2.12) there exists $b, c \in R(f)$ with $<(b, c, 0)>_R = <(b_o, c_o, 0)>_R$. Since $<(b, c, o)>_R \leq <(a^{-s}f, f, 0)>'_R$, we have $0 = (a^{-s}f)^* b + f^*\alpha c = fa^{-s}b + f\alpha c = a^{-s} b + f\alpha fc$. Multiplying on the left by a^s gives $b = -a^s f\alpha fc$, ie. $<(b, c, 0)>_R \leq <(-a^s f\alpha f, f, 0)>_R$. □

If $(a^s - e)f$ is invertible in $S(f)$ then, since a^{-s} is also invertible in $S(f)$, so is $(a^{-s} - e)f = -a^{-s}f(a - e)f$. Also, note that since most of the elements we are working with come from S we often have multiplicative commutativity. However $\alpha \notin S$ and therefore care must be taken.

<u>Claim 9</u>. If $x, y \in A$ with $x \wedge y > 0$ then $x = y$.

<u>Proof</u>. Let $x = <(a^{-s} f, f, 0)>_R$ and $y = <(a^{-k} f, f, 0)>_R$ with $x \wedge y > 0$ and $0 \leq k \leq s \leq n$, s, k odd. Then there exist $q, t \in R$ with $(a^{-s} f, f, 0)\, q = (a^{-k} f, f, 0)t \neq (0, 0, 0)$. Let $r = fq = ft \neq 0$. Then $a^{-s}r = a^{-k}r$ and so $0 = (a^{-k} - a^{-s})r = a^s (a^{-k} - a^{-s})r = (a^{s-k} - e)r = (a^{s-k} - e)fr$. But $0 \leq s - k < n$ therefore unless $s = k$ we know that $(a^{s-k} - e)f$ is invertible in $S(f)$. Since $fr = r \neq 0$, it follows that $s = k$ and $x = y$. □

Claim 10. If $x, y \in A'$ with $x \wedge y > 0$ then $x = y$.

Proof. Let $x = \langle(-a^s f\alpha f, f, 0)\rangle_R$ and $y = \langle(-a^k f\alpha f, f, 0)\rangle_R$ with $x \wedge y > 0$ and $0 \le k \le s < n$, s, k odd. There exist $q, t \in R$ with $(-a^s f\alpha f, f, 0)q = (-a^k f\alpha f, f, 0)t \neq (0, 0, 0)$. Let $r = fq = ft \neq 0$. Then $a^k f\alpha fr = a^s f\alpha fr$ and $0 = (a^s - a^k)f\alpha fr - a^{-k}(a^s - a^k) f\alpha fr = (a^{s-k} - e)f\alpha fr$. But $0 \le s - k < n$ and therefore unless $s = k$ we know that $(a^{s-k} - e) f$ is invertible in $S(f)$. Since $0 = f\alpha fr$ implies $r = 0$, it follows that $s = k$ and $x = y$. □

Claim 11. If $x \in A$ and $y \in A'$ then $x \wedge y = 0$.

Proof. Let $x = \langle(a^{-s}f, f, 0)\rangle_R$ and $y = \langle(-a^k f\, f, f, 0)\rangle_R$ with $0 \le k, s < n$ and so, k odd. Assume $x \wedge y > 0$. Then there exist $q, t \in R$ with $(a^{-s}f, f, 0)q = (-a^k f\alpha f, f, 0)\, t \neq (0, 0, 0)$. Let $r = fq = ft \neq 0$. Then $0 = a^{-s}fq + a^k f\alpha f, t = (a^{-s} + a^k f\alpha f)r = a^{-k}(a^{-s} + a^k f\alpha f)r = (a^{-(s+k)} + f\alpha f)r$. Let $\ell = -2^{-1}(s + k) \in \mathbb{Z}$. Then $0 = (a^\ell a^\ell + f\alpha f)r = r^*(a^\ell a^\ell + f\alpha f)r = (r^*a^\ell)(a^\ell r) + r^*f\alpha fr = (a^\ell r)^*(a^\ell r) + (fr)^*\alpha fr$. This gives $0 = a^\ell r = fr$, but $fr = r \neq 0$, a contradiction. □

The set $A \cup A'$ is closed under the OC inherited from L by the interval $[0, \langle(f, 0, 0), (0, f,)\rangle_R]_L$. Since distinct elements meet to give zero it follows that $A \cup A'$ together with the bounds form $MO_{[n]}$ in this interval. This completes the proof of the proposition and hence of (4.1). □

(4.2) Let $0 \neq e \in {}^*Pr(R)$, if h is odd then $e\alpha^h e \notin Co(R(e))$.

Proof. Assume otherwise, ie. there exists $0 \neq e \in {}^*Pr(R)$ and h odd with $e\alpha^h e \in Co(R(e))$. Since R has prime characteristic p the

unit of R generates the p element field, and therefore e generates the p element field in R(e). By (4.1) $e\alpha^h e$ and $e\beta e$ are of finite order over this field, ie. there exist m, $n > 0$ with $(e\alpha^h e)^m = e = (e\beta e)^n$. It follows from (3.7) that there exists $0 \neq f \in {}^*Pr(R(e))$ so that $f\alpha^n f$ and $f\beta f$ generate a finite field F in R(f) with $*|_F = id_F$. If $(a, b, c) \in F^3$ and $0 = a^*a + b^*f\alpha^h f\, b + c^*f\beta fc = a^*a + b^*f\alpha^\ell\alpha\,\alpha^\ell fb + c^*f\beta fc$, where $\ell = 2^{-1}(h-1)$, then $0 = a = \alpha^\ell fb = fc$. But $0 = \alpha^\ell fb$ implies $0 = \alpha^{-\ell}\alpha^\ell fb = fb = b$ and $fc = c$, so $0 = a = b = c$. This implies that $(f\alpha^n f, f\beta f, *)$ is a form for some OC on the finite projective plane $L(F^3)$, contrary to (1.9). □

(4.3) $p \neq 2$.

<u>Proof</u>. By (4.1) there exists m with $\alpha^m = 1$. Let $m = r2^n$ with r odd. If $p = 2$ then $0 = \alpha^{r2^n} - 1 = (\alpha^r - 1)^{2^n}$. But $(\alpha^r - 1)^* = \alpha^r - 1$, it follows from (3.8) that $\alpha^r - 1 = 0$ contrary to (4.2). □

5. Technicalities II.

Under the assumptions of section 4 we can, from (4.1) and (4.2), assume that there exists $t > 0$ with $\alpha^{2t} = 1$, and from (4.3) that 2 is invertible in R. The element α^t and the ring R may be kept in mind as initial motivation for this section. Aside from the elementary (5.1), the results to be used later on are (5.2) and (5.6).

Throughout this section Q is *regular, 2 is invertible and $q \in Q$ satisfying

(i) q is invertible and *self-adjoint.

(ii) The map $a \xrightarrow{\tau} q^{-1}a^*q$ is an involution on Q.

(iii) $q^2 \in Co(Q)$.

Let $\bar{L}(Q) \xrightarrow{'} \bar{L}(Q)$ be the OC generated by * and let $\bar{L}(Q) \xrightarrow{\#} \bar{L}(Q)$ be the OC generated by τ. Let $L = \bar{L}(Q)$, $S = \{x \in L: \ x = x^{\#'}\}$. $T(x) = x \vee x^{\#'}$ and $\hat{T}(x) = x \wedge x^{\#'}$.

(5.1) $(1)'$ The map $L \xrightarrow{\#'} L$ given by $x \rightarrow x^{\#'}$ is an MOL automorphism, under ', of L.

$(1)^{\#}$ The map $L \xrightarrow{\#'} L$ given by $x \rightarrow x^{\#'}$ is an MOL automorphism, under #, of L.

(2) $T: L \longrightarrow S$, $T(x) = \wedge\{s \in S: \ x \leq s\}$

$(\hat{2})$ $\hat{T}: L \longrightarrow S$, $\hat{T}(x) = \vee\{s \in S: \ s \leq x\}$ $= (T(x'))' = (T(x\#))^{\#}$.

(3) For $x \in L \backslash S$, $\{x, x^{\#'}\}$ generates an MO2, under either of the OC's inherited by the interval $[\hat{T}(x), T(x)]_L$.

(4) $C(L) \subseteq S$.

(5) If $S \neq L$ then there exists $x \notin S$ with $T(x) = 1$, and hence $\hat{T}(x') = 0$.

(6) $Co(q)$ is *regular and $L(Co(q)) \xleftrightarrow{i} L$ onto S.

Proof. If $a \in Q$ then $q^{-1}aq = q\,aq^{-1}$, in particular if $e \in {}^*Pr(Q)$ then so is $q^{-1}eq$. In fact $q^{-1}e\,qa = 0$ if and only if $q^{-1}(1 - e)qa = a$ implies that $(eQ)^{\#} = q^{-1}(1 - e)qQ$. This implies that $((eQ)^{\#})' = (q^{-1}(1 - e)qQ)' = q^{-1}e\,q\,Q$, and that $((eQ)')^{\#} = ((1 - e)Q)^{\#} = q^{-1}e\,q\,Q$. That is, $'^{\#} = {}^{\#'}$.

Re(1). $(x \vee y)^{\#'} = (x^{\#} \wedge y^{\#})' = x^{\#'} \vee y^{\#'}$ and dually $(x \wedge y)^{\#'} = x^{\#'} \wedge y^{\#'}$. Also, $(x^{\#'})' = x^{\#} = (x')^{\#'}$.

Re(2). Since $(x \vee x^{\#'})^{\#'} = x^{\#'} \vee x^{\#'\#'} = x^{\#'} \vee x$, $T: L \longrightarrow S$. If $x \leq s \in S$ then $x^{\#'} \leq s^{\#'} = s$ and $x \vee x^{\#'} \leq s$. $(T(x'))' = (x' \vee x^{\#})' = x \wedge x^{\#'} = \hat{T}(x)$.

Re(3). A series of straighforward calculations shows that $\hat{T}(x)$, x, $x^{\#'}$, $\hat{T}(x) \vee (x' \wedge T(x))$, $\hat{T}(x) \vee (x^{\#} \wedge T(x))$, and $T(x)$ form MO2 in the prescribed interval.

Re(4). If $x \in C(L)$ then x has only one complement in any interval in which it is contained. By (3), $x \in S$.

Re(5). Let $u \in L \backslash S$, and let $x = u \vee \hat{T}(u')$. Then $T(x) = u \vee \hat{T}(u') \vee (u \vee \hat{T}(u'))^{\#'} = u \vee u^{\#'} \vee \hat{T}(u') = T(u) \vee T(u)' = 1$, by (2).

Re(6). It follows from (1) that S is a subalgebra of L as an MOL under $'$, since it is the set of fixed points under the automorphism $L \xrightarrow{\#'} L$. For $e \in {}^*Pr(Q)$ we have the following equivalences

$eQ \in S$

if and only if

$(eQ)^{\#'} = eQ$

if and only if

$q^{-1}eqQ = eQ$

if and only if

$q^{-1}eq = e$, as a result of (3.1.e)

if and only if

$e \in Co(q)$.

It remains to show that $Co(q)$ is *regular.

Since $q = q^*$, $Co(q)$ is closed under *. If $a \in Co(q)$ and $ara = a$ then let $s = 2^{-1}(q^{-1}rq + r)$. We have $qs = 2^{-1}(rq + qr) = 2^{-1}(rq + q^{-1}rq^2) = sq$ and $asa = 2^{-1}(aq^{-1}rqa + ara) = 2^{-1}(q^{-1}araq + a) = 2^{-1}2a = a$. □

(5.2) For $e \in {}^*Pr(Q)$, $T(eQ) = (e + q^{-1}eq)Q$.

<u>Proof.</u> Clearly $(e + q^{-1}eq)Q \leq eQ \vee q^{-1}eqQ = T(eQ)$. We will show the reverse inequality first in the special case that $\hat{T}(eQ) = 0$. Let $(e + q^{-1}eq)Q = (1 - f)Q$, $f \in {}^*Pr(Q)$. Then $ef = -q^{-1}eqf \in eQ \wedge q^{-1}eqQ = \hat{T}(eQ) = 0$. This implies that $0 = ef = q^{-1}eqf$ and so eQ, $q^{-1}eqQ \leq (1 - f)Q$.

For the general case let $\hat{T}(eQ) = gQ$, $g \in {}^*Pr(Q)$, and note that $g \in Co(\{e,q\})$. Since $\hat{T}$ preserves meet, $\hat{T}(e(1 - g)Q) = \hat{T}(eQ \wedge (1 - g)Q) = \hat{T}(eQ) \wedge \hat{T}((1 - g)Q) = gQ \wedge (1 - g)Q = 0$. Therefore $T(e(1 - g)Q) = (e(1 - g) + q^{-1}e(1 - g)q)Q$, ie. there exists $a \in Q$ with $(e(1 - g) + q^{-1}e(1 - g)q)a = 2e(1 - g)$. This gives

$$
\begin{aligned}
& (e + q^{-1}eq)((1 - g)a + g) \\
= \; & (e + q^{-1}eq)(1 - g)a + (e + q^{-1}eq)g \\
= \; & (e(1 - g) + q^{-1}e(1 - g)q)a + (eg + q^{-1}egq) \\
= \; & 2e(1 - g) + 2g = 2e, \text{ and}
\end{aligned}
$$

$eQ \le (e + q^{-1}eq)Q$. By a symmetric argument, or applying $^{\#'}$, $q^{-1}eq \le (e + q^{-1}eq)Q$. □

(5.3) If $\hat{T}(x) = 0$ and $[0, T(x)]_S \subseteq C([0, T(x)]_L)$ then $[0, x]_L$ is Boolean.

<u>Proof</u>. Let $a \in [0, x]_L$. $T(a) \in [0, T(x)]_S \subseteq C([0, T(x)]_L)$, hence $x \wedge T(a) \in C([0, x]_L)$. But $a \le x \wedge T(a) = x \wedge (a \vee a^{\#'}) = a \vee (x \wedge a^{\#'}) \le a \vee (x \wedge x^{\#'}) = a$. □

(5.4) Let $g \in {}^*Pr(Q) \cap Co(Co(q))$ and $e \in {}^*Pr(Q)$ with $gQ \wedge eQ = (1 - g)Q \wedge eQ = 0$. Then $gQ \vee eQ \in S$.

<u>Proof</u>. Let $r = q(eg - ge)q^{-1} + (eg - ge) \in Co(q)$, then $r = rg + r(1 - g) = grg + (1 - g)r(1 - g) = 0$. Let $(eg - ge)Q = (1 - f)Q$, $f \in {}^*Pr(Q)$. Then $0 = f(eg - ge) = -fq(eg - ge)q^{-1}$. Hence $q(1 - f)q^{-1}(eg - ge) = eg - ge$ and $(eg - ge)Q \le ((eg - ge)Q)^{\#'}$. This implies, by (5.1.3), that $(eg - ge)Q \in S$, ie. $f \in Co(q)$. But

$f(eg - ge) = 0$

implies

$feg = fge$

implies

$gef = (feg)^* = (fge)^* = egf$

implies

$gef \in eQ \wedge gQ$

implies

$gef = 0$

implies

$(1 - g)ef = ef$

implies

$ef \in eQ \wedge (1 - g)Q$

implies

$ef = 0.$

This gives $eQ \leq (1 - f)Q$. But $(1 - f)Q \in S \cap [0, gQ \vee eQ]_L$, so $eQ \vee gQ = (1 - f)Q \vee eQ \vee gQ = (1 - f)Q \vee gQ \in S$. □

<u>Corollary</u>. Let $t \in S$, $x \in C([0,t]_S)$ and $0 \neq z \in [0,t]_L$ with $x \wedge z = x' \wedge z = 0$. Then $x \vee z \in S$.

<u>Proof</u>. Let $t = hQ$, $h \in {}^*Pr(Co(q))$, $x = gQ$, $g \in {}^*Pr(Q(h))$ and $e \in {}^*Pr(Q(h))$ with $z = eQ$. The ring $Q(h)$ and the element gh satisfy the assumptions made on Q and q at the beginning of this section. That is, $Q(h)$ is *regular and not of characteristic 2, qh is *self adjoint, invertible, the map $a \rightsquigarrow (qh)^{-1}a^*qh$ is an involution on $Q(h)$ and $(qh)^2 \in Co(Q(h))$.

Define $S(h)$ analogously to S. $\bar{L}(Q(h)) \overset{i}{\mapsto} [0,hQ]_L$ is an isomorphism implies that for $e \in {}^*Pr(Q(h))$ we have

$eQ(h) \in S(h)$

if and only if

$e \in Co(qh)$, by (5.1.6)

if and only if

$e \in Co(q)$

if and only if

$eQ \in S$, again by (5.1.6)

We may apply (5.4) to $Q(h)$, qh, g and e to obtain $gQ(h) \vee eQ(h) \in S(h)$ and consequently $gQ \vee eQ \in S$. □

(5.5) Let $t \in S$. If $C([0, t]_S) \subseteq C([0, t]_L)$ then there exists $0 \neq u \in [0, t]_S$, so that $[0, u]_S = [0, u]_L$.

Proof. Let $x \in C([0, t]_S) \setminus C([0, t]_L)$. Since $x \notin C([0, t]_L)$ there exists $0 \neq y \in [0, t]_L$ with $x \wedge y = x' \wedge y = 0$ (if $x \notin s$ let $y = s \wedge (x \vee s') \wedge (x' \vee s')$). If $z \leq y$ then by the above corollary $x \vee z \in S$. If $w \in [x, x \vee y]_L$ then $w = (x \vee y) \wedge w = x \vee (y \wedge w) \in S$, since $y \wedge w \leq y$. Hence, $[x, x \vee y]_L = [x, x \vee y]_S$. Let $u = x' \wedge (x \vee y)$. □

(5.6) If there exists $0 \neq t \in S$ with $[0, t]_S$ Boolean then there exists $0 \neq u \in L$ with $[0, u]_L$ Boolean.

Proof. There are two cases:

Case 1. $[0, t]_S \subseteq C([0, t]_L)$.

Case 2. $[0, t]_S \nsubseteq C([0, t]_L)$.

If case 1 occurs and equality does not hold then there exists $x \in [0, t]_L$ with $\hat{T}(x) < x$. Let $u = x \wedge (\hat{T}(x))'$. Since $[0, t]_S \subseteq C([0, t]_L)$ we have $[0, T(u)]_S \subseteq C([0, T(u)]_L)$, also $\hat{T}(u) = 0$. By (5.3) $[0,u]_L$ is Boolean. If case 2 occurs then by (5.5) there exists $0 \neq u \in [0,t]_S$ so that $[0,u]_S = [0,u]_L$, in particular $[0,u]_L$ is Boolean. □

6. Technicalities III.

Having developed the necessary tools in section 5 we return now to the setting of section 4 to prove the lemma mentioned in the introduction. Throughout this section $\bar{L}(R^3)$ will be an MOL with orthogonal canonical frame and associated form $(\alpha,\beta,*)$. We also assume that $MO\omega \notin HSP(\bar{L}(R^3))$ and that R has characteristic p, for some prime p. In order to prove the lemma it suffices to show that $\bar{L}(R^3)$ contains a nontrivial Boolean section.

From (4.1) we know that there exists $m > 0$ so that $\alpha^m = 1$. Let $\rho(k) = \alpha^{r2^k}$ where r is odd, $r2^n = m$ and $0 \le k \le n$. For $0 \le k \le n$ and $e \in {}^*Pr(Co(\rho(k)))$ define $R(e,k) = Co(\rho(k)) \cap R(e)$, and for $k \le j \le n$ define $L(e,k,j) = \{aR(e,j) \in \bar{L}(R(e,j)) : a \in R(e,k)\}$. This rather cumbersome notation is necessary in order to distinguish between the lattice of principal right ideals of a ring and its image under certain canonical injections. Our aim is to show the existence of a nonzero $g \in {}^*Pr(R(1,0))$ so that $L(g,0,0)$ is Boolean and then to use (5.6) to push the existence of a nontrivial Boolean section up to $L(1,n,n)$. Successful application of section 5 is a result of

(6.1) Let $0 \le k \le n$, and $0 \ne g \in {}^*Pr(R(1,k))$.

Then

(a) (i) $\rho(k)g$ is invertible and *self-adjoint in $R(g,k)$, in fact $(\rho(k)g)^{-1} = \rho(k)^{-1}g$.

(ii) The map $a \mapsto \rho(k)^{-1}a^*\rho(k)$ is an involution on $R(g,k+1)$.

(iii) $(\rho(k)g)^2 = \rho(k)^2 g \in Co(R(g,k+1))$.

(b) $R(g,k)$ is *regular.

(c) The results (and notation) of section 5 may be applied with $Q = R(g, k+1)$ and $q = \rho(k)g$. In this setting $L = L(g, k+1, k+1)$ and $S = L(g,k, k+1)$.

Proof. Re(a). Since $\rho(k) = \rho(k)^*$ and $\rho(k)$ Co g (i) and (ii) both hold. The map defined in (ii) is clearly additive, of period two and for $a,b \in R(g,k+1)$, $\rho(k)^{-1}(ab)^*\rho(k) = \rho(k)^{-1}b^*\rho(k)$ $\rho(k)^{-1}a^*\rho(k)$. It remains to show that for $a \in R(g,k+1)$ $\rho(k)^{-1}$ $a^*\rho(k)a = 0$ implies $a = 0$. If $k = 0$ then $\rho(k)^{-1}a^*\rho(k)a = 0$ implies $0 = a^*\rho(k)a = (a^*\alpha^t)\,\alpha\,(\alpha^t a) = (\alpha^t a)^*\alpha\,(\alpha^t a)$, where $t = 2^{-1}(r-1)$. Consequently, $0 = \alpha^t a = a$. If $k > 0$ and $\rho(k)^{-1}a^*\rho(k)a = 0$ then $0 = a^*\rho(k)a = (a^*\alpha^t)\,(\alpha^t a) = (\alpha^t a)^*(\alpha^t a)$, where $t = r2^{k-1}$. This gives $0 = \alpha^t a = a$.

Re(b). To show (b) first observe that (c) holds whenever $R(g,k+1)$ is *regular, for *regularity, (i), (ii) and (iii) of (a) are precisely the assumptions made at the beginning of section 5. In particular (5.1.6) tells us that $R(g,k)$ is *regular. Since $R(g,n)$ is *regular the result follows by induction.

Re(c). This follows immediately from (a), (b) and the observation made in the preceding paragraph. □

From (6.1) we make a useful observation.

(6.2) Let $0 \le j < n$ and let $g \in {}^*Pr(R(1,j))$. Then the following are equivalent.

(1) For some $j \le k \le n$, $L(g,j,k) = L(g, j+1, k)$

(2) $*Pr(R(g,j)) = *Pr(R(g,j+1))$

(3) For each $j \le k \le n$, $L(g,j,k) = L(g,j+1, k)$.

Proof. From (6.1) we know that for $j \le \ell$ $L(g,\ell,\ell) \xrightarrow{i} L(g,\ell,\ell+1)$ and that $R(g,\ell)$ is *regular. By a suitable composition we obtain $L(g,\ell,\ell) \xrightarrow{i} L(g,\ell,k)$ for any $\ell \le k \le n$. Since $R(g,\ell)$ is *regular we know that each element of $i(L(g,\ell,\ell))$ in $L(g,\ell,k)$ is uniquely determined by some $e \in *Pr(R(g,\ell))$ as $eR(g,k)$. This establishes the equivalence of (1), (2) and (3). □

With each nonzero $g \in *Pr(R(1,0))$ there is associated an increasing chain of MOL's $(L(g,k,n))_{k=0}^{n}$ and an increasing chain of *regular rings $(R(g,k))_{k=0}^{n}$. We wish to examine and compare the first proper containment in each of these chains. Define $k(g)$ to be the smallest k so that $L(g,k,n) \ne L(g,k+1, n)$ or, if no such k exists, let $k(g) = n$. Define $j(g)$ to be the smallest j so that $R(g,j) \ne R(g,j+1)$ or, if no such j exists, let $j(g) = n$. Since $R(g,j) = R(g, j+1)$ implies $*Pr(R(g,j)) = *Pr(R(g,j+1)$, (6.2) implies that $j(g) \le k(g)$. Our first task is to show that this inequality is strict. Towards this end we need the ring-theoretic.

(6.3) Let $0 \ne a \in R(1,0)$ with $a=a^*$, $aa^{-1} = g$ and let $f \in *Pr(R(g))$ with $faf = 0$. Then $f = 0$.

Proof. Let a and f satisfy the hypotheses of the claim. We may apply (3.7) to the ring $R(g,0)$ with F taken as the p element field, $a_1 = a$ and $a_2 = \rho g$, where $\rho = \rho(0)$. This gives nonzero $e_i \in *Pr(R(g,0)) \cap Co(\{a, \rho g\})$, $i = 1,\ldots,n$, so that

(1) $\sum_{i=1}^{n} e_i = g,\ e_i e_j = \delta_{ij} e_j$

(2) $\{ae_i, \rho e_i\}$ generates a finite field F_i in $R(e_i)$ with $*|_{F_i} = id_{F_i}$.

Since F_i is finite the multiplicative group of nonzero elements is cyclic. Let b_i be a generator for this group. There exist ℓ, k so that $b_i^{\ell} = \rho e_i$ and $b_i^k = -e_i$. We first show that k is even. We have $e_i \alpha^{rk} e_i = (\rho e_i)^k = b_i^{\ell k} = b_i^{k\ell} = (-e_i)^{\ell} \in Co(R(e_i))$ and (4.2) guarantees that rk, and hence k, is even. We will now show that ℓ is odd. Suppose ℓ is even and let $s = 2^{-1}(k - \ell)$, $t = 2^{-1}(r - 1)$. Then $0 = e_i + b^k = e_i{}^*e_i + b^s\alpha^t\alpha\alpha^t b^s = e_i^* e_i + (\alpha^t b^s)^*\alpha(\alpha^t b^s)$. This implies that $0 = e_i = \alpha^t b^s$, a contradiction. Hence ℓ is odd.

For each i let b_i be a generator for the multiplicative group of nonzero elements of F_i and define ℓ_i, h_i so that $b_i^{\ell_i} = \rho e_i$ and $b_i^{h_i} = ae_i$. Let $I_o = \{i:\ h_i \text{ is odd}\}$ and $I_1 = \{i:\ h_i \text{ is even}\}$. For $i \in I_o$ let $m_i = 2^{-1}(h_i - \ell_i)$ and for $i \in I_1$ let $m_i = 2^{-1}h_i$. We have $0 = faf = f(\sum_{i=1}^{n} ae_i)f$

$$= f(\sum_{i\in I_1} ae_i)f + f(\sum_{i\in I_o} ae_i)f$$

$$= f(\sum_{i\in I_1} b_i^{m_i})(\sum_{i\in I_1} b_i^{m_i})f + f(\sum_{i\in I_o} b_i^{m_i})\,\alpha^s\alpha\alpha^s\,(\sum_{i\in I_o} b_i^{m_i})f$$

$$= ((\sum_{i\in I_1} b_i^{m_i})f)^*(\sum_{i\in I_1} b_i^{m_i})f + (\alpha^s(\sum_{i\in I_o} b_i^{m_i})f)^*\alpha\,\alpha^s(\sum_{i\in I_o} b_i^{m_i})f,$$

where $s = 2^{-1}(r - 1)$.

This implies that $0 = (\sum_{i\in I_1} b_i^{m_i})f = (\sum_{i\in I_o} b_i^{m_i})f$ and therefore

that $0 = (\sum_{i=1}^{n} b_i^{m_i})f$

$$= (\sum_{i=1}^{n} b_i^{-m_i})(\sum_{i=1}^{n} b_i^{m_i})f$$

$$= (\sum_{i=1}^{n} e_i)f = gf = f. \qquad \square$$

(6.4) If $0 \neq g \in {}^*Pr(R(1,0))$ then $j(g) < k(g)$.

Proof. If $j(g) = n$ then $\alpha^r g \in Co(R(g))$ contrary to (4.2). Assume $j(g) = k(g) = k < n$. By (6.1.c) we may apply the results and notation of section 5 with $Q = R(g,k+1)$ and $q = \rho(k)g$. By (5.1) there exists $x \in L\backslash S$ with $T(x) = 1$. By (5.2), if $e \in {}^*Pr(Q)$ with $x = eQ$ then $T(x) = (e + q^{-1}eq)Q$. This implies that $e + q^{-1}eq$ is right invertible (in Q) and since it is *self-adjoint it is invertible. It follows that $a^{-1} = qe + eq$ is invertible (with inverse a) and an element of Co(q). Consider the left ideal Qea. Suppose Qea = Q, then there exists $s \in Q$ with sea = g. This gives $ase = aseaa^{-1} = aga^{-1} = g$ which in turn implies that e = g, a contradiction. So there exists a nonzero $f \in {}^*Pr(Q)$ with $Qea = Q(f - g)$. From $0 = eaf$ we obtain $eqaf = eqaf + qeaf = a^{-1}af = f$, and $ef = f = f^* = fe$. This gives $faf = feaf = 0$.

Since $R(g,k) = R(g,0)$, a and f satisfy the hypotheses of (6.3) and we can conclude that f = 0, a contradiction. $\square$

(6.5) Let $0 \neq g \in {}^*Pr(R(1,0))$. If L(g,0,0) is nonBoolean then there exists nonzero $h \in {}^*Pr(R(g,0))$ so that $k(h) \geq k(g)$ and $j(h) > j(g)$.

Proof. Let $0 \neq g \in {}^*Pr(R(1,0))$ and assume L(g,0,0) is nonBoolean and let $j = j(g)$. Since L(g,0,0) is nonBoolean (1.6) guarantees the

existence of $0 \neq h \in {}^*Pr(R(g,0))$ so that $[0, hR(g,0)]_{L(g,0,0)}$ contains M02 and hence a 2-frame. Since $L(h,0,0) \xrightarrow{i} [0, hR(g,0)]_{L(g,0,0)}$ is an isomorphism, and since $L(h,0,0) \xrightarrow{i} L(h, j+1, j+1)$ the ring $R(h, j+1)$ is of order 2.

Consider the automorphism ϕ of $R(h, j+1)$ given by $a \to \rho(j)^{-1} a \rho(j)$. This generates an automorphism Φ of $L(h, j+1, j+1)$ given by $aR(h, j+1) \to \phi(a)R(h, j+1)$. The automorphism Φ is completely determined by the action of ϕ on ${}^*Pr(R(h, j+1))$. But $j < k(g) \leq k(h)$ and (6.2) insures that ${}^*Pr(R(h,j)) = {}^*Pr(R(h, j+1))$. But this implies that ϕ acts identically on ${}^*Pr(R(h, j+1))$ and hence that $\Phi = id_{L(h,j+1,j+1)}$, again by (6.2). Since $R(h, j+1)$ is of order 2, (2.17) applies and $\phi = id_{R(h,j+1)}$. This implies that $R(h,j) = R(h, j+1)$ and therefore that $j < j(h)$. □

<u>Corollary</u>. There exists $0 \neq g \in {}^*Pr(R(1,0))$ so that $L(g,0,0)$ is Boolean.

<u>Proof</u>. Choose g so that $(k(g), \ell(g))$ is maximal with respect to the lexicographic ordering, (6.5) ensures that $L(g,0,0)$ is Boolean. □

We can now prove the desired result.

(6.6) There exists $0 \neq x \in \mathcal{L}(R^3)$ so that $[0,x]_{\mathcal{L}(R^3)}$ is Boolean.

<u>Proof</u>. For any $g \in {}^*Pr(R(1,0))$ we have $L(g,0,0) \xrightarrow{i} L(1,0,0)$, and by the above corollary $L(1,0,0)$ contains a Boolean section. For $k < n$ the map $L(1,k,k) \xrightarrow{i} L(1,k, k+1)$ is an isomorphism so if $L(1,k,k)$ contains a nontrivial Boolean section then so does $L(1,k, k+1)$. Applying (6.1.c) with $Q = R(1, k+1)$ and $q = \rho(k)$ and invoking (5.6) ensures the existence of a nontrivial Boolean section in $L(1, k+1, k+1)$. It follows from the principle of induction that $L(1,n,n) = \mathcal{L}(R)$

contains a nontrivial Boolean section and since $\bar{L}(R) = [0, \langle (0,1,0) \rangle_R]_{\bar{L}(R^3)}$ the proof is complete. $\square$

7. Results

I quote from [3].

"I suspect that a subdirectly irreducible MOL generated by elements a,b,c satisfying the assumptions of lemma 1 and $b' \wedge c' = 0$ is a projective plane. This together with the remainder of the paper would prove the conjecture of the introduction."

These assumptions are that not all of a,b,c are 0, $a \leq b$ and $a \wedge c' = a' \wedge c = b \wedge c = a' \wedge b \wedge c' = b' \wedge (a \vee c) = 0$ and of course the conjecture is the conjecture quoted in section 1. The proof of the first observation of this section is a series of straightforward calculations and left to the reader.

(7.1) The above assumptions together with $b' \wedge c' = 0$ are equivalent to the assumption that $(a, a' \wedge b, b', c)$ is an orthogonal 3-frame.

Every subdirectly irreducible complemented modular lattice L can be embedded in a projective geometry G, see Frink [7]. Thus if L is a subdirectly irreducible MOL with orthogonal canonical frame and G is a projective plane then L is a projective plane and (1.8) ensures that $MO\omega \in HSP(L)$. If G is not a projective plane then it has (geometric) dimension greater than two and is therefore Arguesian [9]. Since L is a sublattice of G, L too is then Arguesian. The coordinatization theorem of Jónsson [9] may now be invoked and we may assume that $L = \bar{L}(R^3)$ with orthogonal canonical frame. This shift from the general situation to the ring-theoretic setting is due to A. Day [6].

Eventually we will want to apply (6.6) to $\bar{L}(R^3)$ and in order to do this we must establish that R has characteristic p for some prime p. Since $\bar{L}(R^3)$ is irreducible it follows from (1.1) and (2.10) that Co(R) is a field. Let $n \in \mathbb{N}$ so that $2n + 1 \leq |Co(R)|$ if Co(R) is finite and let $n = \omega$ if Co(R) is infinite.

(7.2) Let $L = \bar{L}(R^3)$ be a subdirectly irreducible MOL with orthogonal canonical frame. Then $MO_n \in HSP(L)$.

<u>Proof</u>. Let $A = \{<(1,a,0)>_R : 0 \neq a \in Co(R)\}$ and let $A' = \{<(1, \alpha^{-1}a,0)>_R : 0 \neq a \in Co(R)\}$. Suppose $(b,c,0) \in <(1,a,0)>_R$ for $0 \neq a \in Co(R)$, then $b + a^*\alpha\, c = 0$. It follows that $b = -\alpha^{-1}a^{*-1}c$, ie. that $(b,c,0) \in <(1,-\alpha^{-1}a^{*-1},0)>_R$. Therefore $A' = \{x' \wedge <(1,0,0), (0,1,0)>_R : x \in A\}$. Since Co(R) is a field distinct elements of A meet to give zero as do distinct elements of A'.

Assume that there exists $<(1,a,0)>_R \in A$ and $<(1, \alpha^{-1}b,0)>_R \in A'$ with $<(1,a,0)>_R \wedge <(1,\alpha^{-1}b,0)>_R \neq 0$. Then there exists $0 \neq e \in {}^*Pr(R)$ with $ae = \alpha^{-1}be$. It follows that $e\alpha e = ce$ where $c = a^{-1}b \in Co(R)$.

The MOL $\bar{L}(R(e)^3)$ with associated form $(e\alpha e, e\beta e, *)$ is an element of HSP(L). Let $B \subseteq \bar{L}(R(e)^3)$ be defined as $B = \{<(e,ae,0)>_{R(e)} : 0 \neq a \in Co(R)\}$. Let $B' = \{x' \wedge <(e,0,0),(0,e,0)>_{R(e)} : x \in B\}$. Since $e\alpha e = ce$, $c \in Co(R)$, and since $B' = \{<(e,(e\alpha e)^{-1}ae,0)>_{R(e)} : 0 \neq a \in Co(R)\}$ we have $B' = B$. Since Co(R) is a field distinct elements of B meet to give zero. It follows that B together with the bounds forms an MO_k in the interval $[0,<(e,0,0), (0,e,0)>_{R(e)}]_{\bar{L}(R(e)^3)}$ where $2k + 1 = |Co(R)|$.

Otherwise, if $x \in A$ and $y \in A'$ then $x \wedge y = 0$ and it follows that $A \cup A'$ forms MO_k in the interval $[0, <(1,0,0), (0,1,0)>_R]_L$

where $k + 1 = |Co(R)|$. □

(7.3) Let L be a subdirectly irreducible MOL generated by an orthogonal 3-frame. If $MO\omega \notin HSP(L)$ then L contains a nontrivial Boolean section.

Proof. From the above discussion we can assume that $L = \Gamma(R^3)$ with orthogonal canonical frame. By (7.2) R has characteristic p and we can apply (6.6). □

We now list three results from [3].

(7.4) (lemma 2, page 5 [3]) If an MOL L contains elements d,u so that the interval [0,u] is not Boolean and $u \wedge d = u \wedge d' = 0$ then a homomorphic image of a subalgebra of L contains elements a,b,c satisfying the assumptions listed above (7.1).

(7.5) (theorem 1, page 2 [3]) If a is an element of a subdirectly irreducible MOL and if the interval [0,a] is Boolean then a is either an atom or zero.

(7.6) (lemma 3, page 5, [3]) If a subdirectly MOL L contains an atom then it is either an MOn ($n \geq 1$) or it has a projective plane as a homomorphic image of a subalgebra.

The main result may now be proved.

(7.7) Every variety of MOL's which is different from all the [MOn], $0 \leq n \leq \omega$, contains $MO\omega$.

Proof. Let us recall the definition of the commutator $\hat{\gamma}(x_1,\ldots,x_n)$ in an MOL (see [3], [11]), $\gamma(x_1,\ldots,x_n) = \bigwedge_{\alpha} \bigvee_{i=1}^{n} x_i^{\alpha(i)}$ where α runs over all maps from $\{1,2,\ldots,n\}$ into $\{0,1\}$, $x^0 = x$ and $x^1 = x'$. The argument given here is an extension of the one given on page 6 of [3] and is due to G. Bruns.

Assume k is a variety of MOL's which is different from all the [MOn], $0 \leq n \leq \omega$, then there exists $L \in k$ and $x,y,z \in L$ so that $\gamma(x,\gamma(y,z)) \neq 0$, since $\gamma(x,\gamma(y,z))$ holds in a subdirectly irreducible MOL if and only if it is an MOn. Let S be the subalgebra of L generated by $\{x,y,z\}$. S has a subdirectly irreducible image M which is generated by a set $\{s,t,u\}$ satisfying $\gamma(s,\gamma(t,u)) \neq 0$. The element $\gamma(s,t,u)$ commutes with each of s,t,u and is therefore central in M. Since M is irreducible $C(M) = \{0,1\}$. If $\gamma(s,t,u) = 0$ then $\gamma(t,u) = 0$ and $\gamma(s,\gamma(t,u)) = 0$ (these computations are all easy to check), a contradiction. Therefore $\gamma(s,t,u) = 1$. Since $\gamma(t,u) \neq 1$ (otherwise $\gamma(s,\gamma(t,u)) = 0$) not all of $u \wedge t$, $u' \wedge t$, $u \wedge t'$, $u' \wedge t'$ are zero and we will assume that $u \wedge t \neq 0$. From $\gamma(s,t,u) = 1$ it follows that $s \wedge t \wedge u = s' \wedge t \wedge u = 0$.

If $[0,t \wedge u]$ is not Boolean then it follows from (7.4) that there exist elements a_o,b,c not all zero satisfying the assumptions listed above (7.1). If we consider the interval $[0,b \vee c]_M$ and replace a_o with $a = a_o \wedge (b \vee c)$ we then have the additional assumption that $b' \wedge c' = 0$. Let A be the subalgebra of $[0,b \vee c]_M$ generated by a,b,c. Since not all of a,b,c are zero A has a nontrivial subdirectly irreducible image B generated by elements satisfying the above assumptions or, equivalently, by an orthogonal 3-frame. It follows from (7.3) that $MO\omega \in HSP(B)$ or B contains a nontrivial Boolean section.

Therefore $MO\omega \in HSP(B)$, B contains a nontrivial Boolean section or $[0,t \wedge u]_M$ is Boolean. In any case $MO\omega \in HSP(L)$ or there exists a subdirectly irreducible algebra in HSP(L) generated by an orthogonal 3-frame and, by (7.5), containing an atom. Since this algebra contains

a nontrivial 3-frame it cannot be an MOn and by (7.6) must contain a projective plane as a homomorphic image of a subalgebra. By (1.8) $MO\omega \in HSP(L)$. □

8. Concluding remarks.

We restate the main result of this thesis.

<u>Theorem</u>. Every variety of MOL's which is different from all the $[MOn]$, $0 \leq n \leq \omega$, contains $[MO\omega]$.

There remain two closely related open questions. First of all, is the conjecture quoted in section 1 true? Secondly, apart from the material presented in section 7 the proof of the theorem is complicated and ungainly. Is there an elegant proof? I believe that both of these questions can be profitably attacked from the purely ring-theoretic point of view.

BIBLIOGRAPHY

1. F. Anderson and K. Fuller, Rings and categories of modules, Springer Verlag, New York, 1974.

2. R. Baer, Polarities in finite projective planes, Bull. Amer. Math. Soc. 52(1946), 77-93.

3. G. Bruns, Varieties of modular ortholattices, Houston Jour. of Math. 9(1983), 1-7.

4. P. Crawley and R.P. Dilworth, Algebraic theory of lattices, Prentice Hall, Englewood Cliffs, New Jersey, 1973.

5. A. Day, Equational theories of projective geometries, Contributions to Lattice Theory (Szeged, 1980), 227-316, Colloq. Math. Soc. János Bolya. 33, North-Holland Amsterdam-New York, 1983.

6. _____, *Regular rings and modular ortholattices, talk given at the Ontario Mathematics Meeting, Lakehead University, Thunder Bay, Ontario, 1982.

7. O. Frink, Complemented modular lattices and projective geometries of infinite dimension, Trans. Amer. Math. Soc. 60(1946), 452-467.

8. K.R. Goodearl, von Neumann regular rings, Pitman, London, San Fransisco, 1979.

9. B. Jónsson, Representations of complemented modular lattices, Trans. Amer. Math. Soc. 97(1960).

10. _____, Algebras whose congruence lattices are distributive, Math. Scand., 21(1967), 110-121.

11. G. Kalmbach, Orthomodular lattices, Academic Press, New York, 1984.

12. J. von Neumann, Continuous Geometry, Princeton University Press, Princeton, New Jersey, 1960.

13. L.A. Skornyakov, Complemented modular lattices and regular rings, Oliver and Boyd, London (1964).