

Complemented modular lattices derived from non-associative rings

By ICHIRO AMEMIYA ¹⁾ in Tokyo (Japan) and ISRAEL HALPERIN in Kingston (Canada)

§ 1. Introduction

K. D. FRYER and the authors proved in [6] and [2]: if L is a complemented modular lattice and if a normalized frame of order 3 in L satisfies the conditions (3. 1. 7), (5. 1. 1), (5. 1. 2) of [6] (see Remark 1 following Theorem 4 in § 5 below) then L can be coordinatized. The coordinatization uses a ring²⁾ \mathfrak{R} with unit satisfying:

(P_1) : \mathfrak{R} is *idempotent-associative*, i. e., $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ if any of α, β, γ is idempotent.

(P_2) : \mathfrak{R} is *regular*, i. e., for each α there exists a *left partial inverse* β (this means: $\beta\alpha$ is idempotent and $\alpha(\beta\alpha) = \alpha$) and a *right partial inverse* β' (this means: $\alpha\beta'$ is idempotent and $(\alpha\beta')\alpha = \alpha$).³⁾

(P_3) : In \mathfrak{R} , $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ if any of $\alpha\beta, \beta\gamma$ is idempotent.⁴⁾

In this paper we shall make use of the following property which is stronger than (P_2) but which, in the presence of (P_1) and (P_2) , is easily seen to be implied by (P_3) .

(\bar{P}_2) : For every α in \mathfrak{R} , $(\alpha)_l = \mathfrak{R}\alpha$ and $(\alpha)_r = \alpha\mathfrak{R}$; for each α there exists β and an idempotent e such that $\alpha e = \alpha$, $\beta\alpha = e$ and for every

¹⁾ Post-doctorate Fellow (of the National Research Council of Canada) at Queen's University.

²⁾ Ring means non-associative ring, i. e., an additive group \mathfrak{R} with a left and right distributive multiplication; e is idempotent means $ee = e$. A subgroup I is a left ideal of \mathfrak{R} if $\mathfrak{R}I \subset I$; by duality, a right ideal if $I\mathfrak{R} \subset I$ (henceforth, it is understood that every definition and statement in this paper is to include its dual). The smallest left ideal containing $\Lambda \subset \mathfrak{R}$ exists (obviously); it is denoted by $(\Lambda)_l$, by $(\alpha)_l$ if $\Lambda = (\alpha)$. Obviously, $\mathfrak{R}\alpha \subset (\alpha)_l$.

³⁾ VON NEUMANN called an associative ring *regular* if for each α , there exists β with $\alpha\beta\alpha = \alpha$ (then $\alpha\beta, \beta\alpha$ are both idempotent).

⁴⁾ The reader can verify easily that $(P_1), (P_2), (P_3)$ together imply the other condition on \mathfrak{R} proved in [6], namely: $\beta\alpha$ idempotent with $\alpha = \alpha(\beta\alpha)$ implies that $\alpha\beta$ is idempotent.

$\gamma: \alpha\gamma = 0$ implies $e\gamma = 0$; and for each α there exists β' and idempotent e' such that $e'\alpha = \alpha$, $\alpha\beta' = e'$ and for every $\gamma: \gamma\alpha = 0$ implies $\gamma e' = 0$.

Although it is not needed for the rest of this paper, we shall show below (see § 4, Corollary to Theorem 2) that in the presence of (P_1) and (P_2) , the property (P_3) is equivalent to:

$(P_3)'$: \mathfrak{R} is *alternative*, i. e., the associator $[\alpha, \beta, \gamma] = (\alpha\beta)\gamma - \alpha(\beta\gamma)$ vanishes whenever two of α, β, γ coincide.

In the present paper we consider an arbitrary ring \mathfrak{R} and we define \mathfrak{R}^a to be the set of associating elements⁵⁾ in \mathfrak{R} (our \mathfrak{R}^a is denoted as \mathfrak{R}_0 in [10] and called there the "Kern" of \mathfrak{R} ; earlier, it was denoted as N by BRUCK and KLEINFELD [3] and called the "Nucleus"). As we show in Lemma 1.1, \mathfrak{R}^a is an associative subring of \mathfrak{R} . We define $L = L(\mathfrak{R})$ to be the set of all (e) , with e idempotent, ordered by set inclusion. Obviously, L has (0) for zero and, if \mathfrak{R} has a right unit,⁶⁾ \mathfrak{R} for unit element. $M_n(\mathfrak{R})$ will denote the ring of all $n \times n$ matrices (α^{ij}) with all α^{ij} in \mathfrak{R} and $S_n = S_n(\mathfrak{R})$ will denote the set of such (α^{ij}) with $\alpha^{ij} = 0$ for $i < j$ and all α^{ii} associating. Then $S_1 = \mathfrak{R}^a$ and the reader can verify by obvious calculation that for $n = 1, 2$ or 3 , S_n is an associative ring (with a right unit if \mathfrak{R} has a right unit).

For $n = 1, 2$ or 3 we define $L_n = L_n(\mathfrak{R})$ to be $L(S_n(\mathfrak{R}))$. If \mathfrak{R} is idempotent-associative, \mathfrak{R} and \mathfrak{R}^a have the same idempotents (obviously) and then L and $L_1 = L(\mathfrak{R}^a)$ are isomorphic (obviously).

The main results of this paper are:

(1) If \mathfrak{R} is idempotent-associative and semi-regular⁷⁾ then L is a relatively complemented lattice⁸⁾ with zero, complemented if \mathfrak{R} has a right unit, modular if \mathfrak{R} is regular (§ 3, Theorem 1).

(2) If \mathfrak{R} is idempotent-associative and regular then L_2 is a relatively complemented, modular lattice with zero, complemented with a homogeneous basis of order 2 if \mathfrak{R} has a right unit (§ 5, Theorem 3).

⁵⁾ δ is called *associating* if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ whenever any of α, β, γ coincide with δ .

⁶⁾ An idempotent e in \mathfrak{R} is a *right unit* for $\Lambda \subset \mathfrak{R}$ if $a e = a$ for all a in Λ , a *unit* for Λ if $a e = e a = a$ for all a in Λ .

⁷⁾ See § 3 for definition of "semi-regular"; every idempotent-associative regular ring is necessarily semi-regular.

⁸⁾ We call an arbitrary ordered set *relatively complemented* if: whenever $a \leq b \leq c$ there exists some d (called a *relative complement of b in c over a*, denoted $[c-b]_a$) such that a is the meet of d, b and c is the union of d, b . When a is a zero element we write $[c-b]$ and call it a *relative complement of b in c*. In a lattice we denote union and meet of two elements a, b by $a + b, ab$ respectively; if the lattice has a zero element 0 and $ab = 0$ we sometimes write $a \oplus b$ in place of $a + b$.

(3) If \mathfrak{R} is idempotent-associative and (\bar{P}_2) holds then L_3 is a relatively complemented modular lattice with zero, complemented with a homogeneous basis of order 3 if \mathfrak{R} has a right unit (§ 5, Theorem 3).

(4) If \mathfrak{R} is idempotent-associative and regular and (P_3) holds (equivalently, \mathfrak{R} is alternative) and \mathfrak{R} has a right unit, then every normalized frame of order 3 for L_3 does satisfy (3. 1. 7), (5. 1. 1), (5. 1. 2) of [6]; and if \mathfrak{R} is the coordinatizing ring of some L' , as defined in [6], then L_3 is isomorphic to L' .⁹⁾ Moreover the construction of [6], applied to a suitable normalized frame for L_3 will give a coordinatizing ring which is isomorphic to the original \mathfrak{R} ¹⁰⁾ (§ 5, Theorem 4).

We recall that the original construction of a relatively complemented modular lattice with zero L_n , for every integer $n \geq 1$, made by J. VON NEUMANN, required \mathfrak{R} to be associative and regular ([9], Part II, Theorems 2. 14 and 2. 4; [5], § 3. 6).

§ 2 contains some preliminary lemmas of general interest which are required in the other sections.

§ 3 contains the proof of (1). Here Lemma 3. 2 permits us to adapt the usual arguments for the associative, regular case.

§ 5 contains the proofs of (2), (3), (4). Lattice character of L_2 and L_3 is obtained without difficulty but modularity is established only with the help of an embedding theorem for rings by means of which we can reduce the discussion to rings having no idempotents other than 0, 1. The embedding theorem for rings is given in § 4.

§ 2. Preliminaries

By easy calculation the reader can verify the identity:¹¹⁾

$$(2. 1) \quad \alpha[\beta, \gamma, \delta] + [\alpha, \beta\gamma, \delta] + [\alpha, \beta, \gamma]\delta = [\alpha\beta, \gamma, \delta] + [\alpha, \beta, \gamma\delta]$$

and hence

$$(2. 2) \quad \alpha[\beta, \gamma, \delta] = [\alpha\beta, \gamma, \delta] \quad \text{if } \alpha \text{ is associating,}$$

$$(2. 3) \quad [\alpha, \beta\gamma, \delta] = [\alpha, \beta, \gamma\delta] \quad \text{if } \gamma \text{ is associating.}$$

⁹⁾ We actually show that L_3 is isomorphic to the lattice L_3^M of M -sets of vectors used in [2] and shown there to be isomorphic to the given L' . (M -sets and L_3^M are defined in § 5 below.)

¹⁰⁾ Whether *all* normalized frames of order 3 for a fixed L_3 give isomorphic coordinatizing rings is not known, even if \mathfrak{R} is associative. However this isomorphism does hold if \mathfrak{R} has "no associative part", i. e., if $B = (0)$ in Theorem 2 (from the embedding construction used in Theorem 3 and the Remark following the proof of Lemma 5. 3 (i)).

¹¹⁾ Given as (2) on page 125 of [12].

We let $A = A(\mathfrak{R})$ denote the set of α in \mathfrak{R}^a for which $\alpha\mathfrak{R}, \mathfrak{R}\alpha \subset \mathfrak{R}^a$ and we let B denote the set of β such that $\beta\alpha = \alpha\beta = 0$ for all α in A .

Lemma 2.1. *A and B are ideals of \mathfrak{R} , \mathfrak{R}/B is an associative ring, \mathfrak{R}^a is an associative subring of \mathfrak{R} and if \mathfrak{R} is idempotent-associative and regular then \mathfrak{R}^a is regular.*

Proof. To show that A is an ideal we need only prove that α in A implies $\beta\alpha\gamma$ is associating for all β, γ . But (2.2) implies for all δ, ρ :

$$[\beta\alpha\gamma, \delta, \rho] = (\beta\alpha)[\gamma, \delta, \rho] = \beta[\alpha\gamma, \delta, \rho] = 0,$$

and by duality, $[\delta, \rho, \beta\alpha\gamma] = 0$. Also, (2.3) implies:

$$[\delta, \beta\alpha\gamma, \rho] = [\delta, \beta, \alpha\gamma\rho] = [\delta, \beta\alpha, \gamma\rho] = 0.$$

Thus $\beta\alpha\gamma$ is associating, so A is an ideal.

Next, B is a right ideal; for if β is in B , and α is in A and γ is arbitrary,

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma = 0, \quad (\beta\gamma)\alpha = \beta(\gamma\alpha) = 0.$$

By duality, B is also a left ideal, hence an ideal.

Next, (2.2) and its dual show that for α in A and arbitrary β, γ, δ :

$$\alpha[\beta, \gamma, \delta] = 0 = [\beta, \gamma, \delta]\alpha,$$

so $[\beta, \gamma, \delta]$ is in B . Thus all associators in \mathfrak{R}/B are zero, which means \mathfrak{R}/B is an associative ring.

Next, α and β both associating clearly implies: $\alpha - \beta$ is associating and, from (2.2), the dual of (2.2) and (2.3), $\alpha\beta$ is also associating. Thus \mathfrak{R}^a is a subring, obviously associative.

Finally, suppose \mathfrak{R} is idempotent-associative and regular. If $\beta\alpha = e$ (idempotent) and $\alpha = \alpha e$ and α is associating, then $\alpha\beta$ is idempotent, for $(\alpha\beta)(\alpha\beta) = (\alpha\beta\alpha)\beta = \alpha\beta$. Now $(e\beta)\alpha = e$ and $e\beta$ is associating, for (2.2) and (2.3) show:

$$[e\beta, \gamma, \delta] = e[\beta, \gamma, \delta] = \beta[\alpha\beta, \gamma, \delta] = 0,$$

$$[\gamma, e\beta, \delta] = [\gamma, \beta(\alpha\beta), \delta] = [\gamma, \beta, \alpha\beta\gamma] = [\gamma, \beta\alpha, \beta\delta] = 0,$$

$$[\gamma, \delta, e\beta] = [\gamma, \delta\beta\alpha, \beta] = [\gamma, \delta\beta, \alpha\beta] = 0,$$

since $\alpha\beta, \beta\alpha$ are idempotent. Thus \mathfrak{R}^a is regular.

Lemma 2.2. *Suppose \mathfrak{R} is idempotent-associative. Then if e is idempotent, $(e)_1 = \mathfrak{R}e$ (obviously). If h, e, f are idempotents with $\mathfrak{R}h \subset \mathfrak{R}e \subset \mathfrak{R}f$ then there exist orthogonal idempotents¹²⁾ e_i ($i = 1, 2, 3$) with $\mathfrak{R}h = \mathfrak{R}e_1$, $\mathfrak{R}e = \mathfrak{R}(e_1 + e_2)$, $\mathfrak{R}f = \mathfrak{R}(e_1 + e_2 + e_3)$.*

¹²⁾ α, β orthogonal means: $\alpha\beta = \beta\alpha = 0$.

Proof. $\mathfrak{R}h \subset \mathfrak{R}e \subset \mathfrak{R}f$ implies $e = ef$, $h = he = hf$. The lemma holds with $e_1 = feh$, $e_2 = fe - e_1$, $e_3 = f - e_1 - e_2$.

Corollary. If \mathfrak{R} is idempotent-associative then L is relatively complemented.

Proof. In Lemma 2.2, $\mathfrak{R}(e_1 + e_3)$ is a relative complement of $\mathfrak{R}(e_1 + e_2)$ in $\mathfrak{R}(e_1 + e_2 + e_3)$ over \mathfrak{R}_{e_1} .

Lemma 2.3. Suppose \mathfrak{R} is idempotent-associative. Then $\alpha - \alpha f$ is an idempotent whenever f is an idempotent such that $(\alpha^2 - \alpha)f = \alpha^2 - \alpha$ and $f\alpha f = f\alpha$.

Proof. $(\alpha^2 - \alpha)f = \alpha^2 - \alpha$ implies $\alpha^2 - \alpha^2 f = \alpha - \alpha f$. Now $(\alpha - \alpha f)(\alpha - \alpha f) = \alpha^2 - \alpha f\alpha - \alpha^2 f + \alpha f\alpha f = (\alpha^2 - \alpha^2 f) + \alpha(f\alpha f - f\alpha) = \alpha - \alpha f$.

Corollary. Suppose \mathfrak{R} is an idempotent-associative regular ring and suppose I is an ideal of \mathfrak{R} . If either

- (i) every idempotent in \mathfrak{R} is in the centre¹³⁾ of \mathfrak{R} or
- (ii) $I = A$,

then \mathfrak{R}/I is also idempotent-associative and every idempotent in \mathfrak{R}/I is of the form $e + I$ with e idempotent.

Proof. Suppose $\alpha + I$ is idempotent in \mathfrak{R}/I . Then $(\alpha + I)(\alpha + I) = \alpha + I$, hence $\alpha^2 - \alpha$ is in I . Since \mathfrak{R} is regular there is an idempotent f such that: $(\alpha^2 - \alpha)f = \alpha^2 - \alpha$ and $f = \gamma(\alpha^2 - \alpha)$ for some γ .

Now f is in the ideal I (since $\alpha^2 - \alpha$ is in this ideal), then also $\beta f, f\beta$ are in I for all β .

In case (i) $f\alpha f = f\alpha$. In case (ii) all $f\beta, \beta f$ are associating (by the definition of A) so in this case also

$$\begin{aligned} f\alpha f &= ff\alpha f = (f\gamma)(\alpha^2 - \alpha)(\alpha f) = (f\gamma)\alpha(\alpha(\alpha f)) - (f\gamma)\alpha(\alpha f) = \\ &= (f\gamma)\alpha((\alpha^2 - \alpha)f) = (f\gamma)\alpha(\alpha^2 - \alpha) = (((f\gamma)\alpha)\alpha) - ((f\gamma)\alpha)\alpha = \\ &= (f\gamma)(\alpha^2 - \alpha)\alpha = ff\alpha = f\alpha. \end{aligned}$$

Thus, in both cases, Lemma 2.3 shows that $e = \alpha - \alpha f$ is idempotent. Since αf is in I , $\alpha + I = e + I$. This means: every idempotent in \mathfrak{R}/I is of the form $e + I$ with e idempotent. This implies that \mathfrak{R}/I is idempotent-associative.

Lemma 2.4. Suppose \mathfrak{R} is idempotent-associative. Then $e\alpha - \alpha e$ is in A for every α and every idempotent e .

¹³⁾ e is in the centre of \mathfrak{R} means: $e\beta = \beta e$ for all β in \mathfrak{R} .

Proof. For any δ in \mathfrak{R} , $e + e\delta - e\delta e$ and $e + \delta e - e\delta e$ are idempotents and their difference $e\delta - \delta e$ is associating. Now suppose $\delta = e\delta$ and $\delta e = 0$; then $\delta = e\delta - \delta e$ is associating, and also for arbitrary β ,

$$\delta\beta = \delta(\beta e - e\beta) + e(\delta\beta) - (\delta\beta)e$$

and

$$\beta\delta = (\beta e - e\beta)\delta + e(\beta\delta) - (\beta\delta)e$$

are associating; so δ is in A . This applies in particular to $\delta = e\alpha - e\alpha e$ so $e\alpha - e\alpha e$ is in A . By duality, $\alpha e - e\alpha e$ is in A . Hence their difference $e\alpha - \alpha e$ is in A .

Corollary. If \mathfrak{R} is idempotent-associative and regular, \mathfrak{R}/A is idempotent-associative and has all its idempotents in its centre.

Proof. By the Corollary to Lemma 2.3 every idempotent in \mathfrak{R}/A is of the form $e + A$. Now $(e + A)(\alpha + A) - (\alpha + A)(e + A) = (e\alpha - \alpha e) + A = A$.

Lemma 2.5. Suppose \mathfrak{R} is a ring with unit. Then

(i) \mathfrak{R} is a division ring without zero divisors¹⁴) if and only if (\bar{P}_2) holds and \mathfrak{R} has no idempotents other than 0, 1, and

(ii) \mathfrak{R} is an alternative division ring if and only if it is regular and (P_3) holds and \mathfrak{R} has no idempotents other than 0, 1.

Proof. The reader can verify easily that (i) follows from the definitions.

(ii) is easily transformed into the now well known statement that a ring is a Moufang division ring if and only if it is an alternative division ring ([12]; [8], § II; [10], p. 161, Theorem 4). (ii) is required by us only to prove the Corollary to Theorem 2, which is itself not required for the rest of this paper.

§ 3. Semi-regular rings

A right unit e for $A \subset \mathfrak{R}$ is called a *left idempotent* for A if $ef = e$ for every right unit f for A (if \mathfrak{R} is idempotent-associative, this is equivalent to: $\mathfrak{R}e$ is the smallest element in L which contains A).

\mathfrak{R} is called *left semi-regular* if every α in \mathfrak{R} possesses a left idempotent, *semi-regular* if it is also right semi-regular. If \mathfrak{R} is idempotent-associative

¹⁴) A ring is a division ring means: every equation $\alpha\beta = \gamma$ can be solved for β if $\alpha \neq 0$ and for α if $\beta \neq 0$; without zero divisors means: $\alpha\beta = 0$ implies α or β is 0. An alternative division ring means: an alternative division ring without zero divisors (then it must have a unit, see [10], page 161). A ring is a *Moufang ring* if it has a unit and for each $\alpha \neq 0$, there exist β_1, β_2 such that: $\beta_1\alpha = \alpha\beta_2 = 1$ and $\gamma = \beta_1(\alpha\gamma) = (\gamma\alpha)\beta_2$ for every γ (then necessarily, $\beta_1 = \beta_2 = \beta$ is unique).

tive, \mathfrak{R} and \mathfrak{R}^a have the same idempotents (obviously) and \mathfrak{R} left semi-regular implies \mathfrak{R}^a is left semi-regular (obviously).

If \mathfrak{R} is idempotent-associative and regular then each $(\alpha)_i$ is of the form $\mathfrak{R}e$ which implies \mathfrak{R} is left semi-regular; by duality, \mathfrak{R} is also right semi-regular, hence semi-regular.

Lemma 3.1. *Suppose \mathfrak{R} is idempotent-associative and that every finite subset of \mathfrak{R} has a right unit. If some $\alpha - ae$ has a left idempotent with e idempotent then α also has a left idempotent provided that:*

$$(3.1) \quad \alpha \in \mathfrak{R}g \text{ implies } e \in \mathfrak{R}g \text{ for every idempotent } g.$$

Proof. Let f be a left idempotent for $\alpha - ae$. We shall show that $fe = 0$.

In fact, if g is a right unit for $\{\alpha, e\}$, then $fg = f$, $g - ge$ is idempotent and $(\alpha - ae)(g - ge) = \alpha - ae$ (i. e., $g - ge$ is a right unit for $\alpha - ae$), so $f(g - ge) = f$, hence $fe = 0$.

We now show that $h = e + f - ef$ is a left idempotent for α . In fact, $hh = h$ and $ah = ae + (\alpha - ae)f = ae + \alpha - ae = \alpha$; if g is any idempotent with $ag = \alpha$ then, by hypothesis, $eg = e$, $(\alpha - ae)g = \alpha - ae$, hence $fg = g$ and finally $hg = h$.

Remark. (3.1) is certainly satisfied if e has the form $e = \beta\alpha$.

Lemma 3.2. *Suppose \mathfrak{R} is idempotent-associative and left semi-regular. If e is a left idempotent for α then for every idempotent f , $\alpha f = 0$ implies $ef = 0$.*

Proof. Let g be a left idempotent for $e + f - fe$. Then $\alpha = \alpha(e + f - fe) \in \mathfrak{R}(e + f - fe) \subset \mathfrak{R}g$. Hence $\alpha = \alpha g$, $e = eg$ (since e is a left idempotent for α), and

$$fg = (e + f - fe)g - (e - fe)g = (e + f - fe) - (e - fe) = f.$$

Then $g - gf$ is a right unit for α ($g - gf$ is idempotent and $\alpha(g - gf) = \alpha - \alpha f = \alpha$) so $e(g - gf) = e$, i. e., $ef = 0$.

Remark. If (\bar{P}_2) also held, then in Lemma 3.2, $\alpha\beta = 0$ would imply $e\beta = 0$ for all β .

Theorem 1. *Suppose \mathfrak{R} is idempotent-associative and semi-regular. Then L is a relatively complemented lattice with zero (complemented if \mathfrak{R} has a right unit) and the lattice meet of $\mathfrak{R}e$, $\mathfrak{R}f$ in L coincides with their set intersection.*

If \mathfrak{R} is also regular, then L is modular.

Proof. This theorem is easily verified since Lemma 2.2 holds and for arbitrary idempotents e, f :

(i) the least element in L containing $\mathfrak{R}e$ and $\mathfrak{R}f$ is precisely $\mathfrak{R}(e+g-eg)$ where g is any left idempotent for $f-fe$;

(ii) the greatest element in L contained in both $\mathfrak{R}e$ and $\mathfrak{R}f$ is precisely $\mathfrak{R}(f-gf)$ where g is any right idempotent for $f-fe$ and this greatest element coincides with the set intersection $\mathfrak{R}e \cap \mathfrak{R}f$;

(iii) if \mathfrak{R} is regular, the least element in (i) coincides with $\mathfrak{R}e + \mathfrak{R}f$ and L is a sublattice of the modular lattice \mathfrak{L} of all left ideals of \mathfrak{R} .

Indeed, in (i) $f-fe = (f-fe)g$ implies $f = fe + (f-fe)g$ and, by Lemma 3.2, $(f-fe)e = 0$ implies $ge = 0$. Hence, $e+g-eg$ is idempotent. Then $e = e(e+g-eg)$, $f = (fe+fg-feg)(e+g-eg)$, so $\mathfrak{R}(e+g-eg) \supset \mathfrak{R}e, \mathfrak{R}f$. On the other hand, any element of L which contains $\mathfrak{R}e, \mathfrak{R}f$ must also contain $f-fe$, hence g (g is a left idempotent for $f-fe$ so if h is idempotent and $(f-fe)h = f-fe$ then $g = gh \in \mathfrak{R}h$), and so it must contain $e+g-eg$, hence $\mathfrak{R}(e+g-eg)$ too.

In (ii), $f(f-fe) = f-fe$, hence $fg = g$ since g is a right idempotent for $f-fe$. This implies that $f-gf$ is an idempotent. But $g(f-fe) = f-fe$ implies that $f-gf = (f-gf)e$ so $\mathfrak{R}(f-gf) \subset \mathfrak{R}e \cap \mathfrak{R}f$. But if α is any element in $\mathfrak{R}e \cap \mathfrak{R}f$, α possesses a left idempotent h and h is in $\mathfrak{R}e \cap \mathfrak{R}f$. Then $h(f-fe) = h-h = 0$. This implies $hg = 0$ by the dual of Lemma 3.2, so $\alpha g = (\alpha h)g = \alpha(hg) = 0$ and $\alpha(f-gf) = \alpha f - 0 = \alpha$, i. e., α is in $\mathfrak{R}(f-gf)$.

(iii) If \mathfrak{R} is regular then in (i) above, g can be chosen to be of the form $\alpha(f-fe)$ for some α . Then $\mathfrak{R}(e+g-eg)$, which is the union of $\mathfrak{R}e$ and $\mathfrak{R}f$ in L , is contained in $\mathfrak{R}e + \mathfrak{R}f$. On the other hand, this union obviously contains $\mathfrak{R}e + \mathfrak{R}f$, so they coincide. Since $\mathfrak{R}e + \mathfrak{R}f$ is the union of $\mathfrak{R}e$ and $\mathfrak{R}f$ in \mathfrak{L} , $\mathfrak{R}e$ and $\mathfrak{R}f$ have the same union in L and in \mathfrak{L} . By (ii) above, $\mathfrak{R}e$ and $\mathfrak{R}f$ have the same lattice meet in L and in \mathfrak{L} . This proves (iii).

Corollary 1. Suppose \mathfrak{R}_1 is a subring of an idempotent-associative semi-regular ring \mathfrak{R} and suppose that for each α in \mathfrak{R}_1 there exist idempotents in \mathfrak{R}_1 which are right and left idempotents respectively, for α in \mathfrak{R} . Then $L(\mathfrak{R}_1)$ is isomorphic to a sublattice of $L(\mathfrak{R})$ under the mapping: $\mathfrak{R}_1 e \rightarrow \mathfrak{R}e$ for idempotents e in \mathfrak{R}_1 .

Proof. Clearly, \mathfrak{R}_1 is idempotent-associative and semi-regular. If e, f are in \mathfrak{R}_1 then (i) and (ii) of the proof of Theorem 1 show that there are idempotents g, h in \mathfrak{R}_1 such that the union and meet of $\mathfrak{R}e$ and $\mathfrak{R}f$ are $\mathfrak{R}g, \mathfrak{R}h$ respectively; at the same time, those of $\mathfrak{R}_1 e$ and $\mathfrak{R}_1 f$ are $\mathfrak{R}_1 g, \mathfrak{R}_1 h$ respectively. It follows that the given mapping is a lattice isomorphism.

Corollary 2. *If \mathfrak{R} is idempotent-associative and left semi-regular, then every finite subset of \mathfrak{R} has a right unit, and every finite subset of $S_n(\mathfrak{R})$ has a right unit.*

Proof. The proof of (i) in Theorem 1 holds for this \mathfrak{R} . Now suppose each α_i has right unit e_i ($i=1, \dots, m$) and let $\mathfrak{R}e$ be the union of the $\mathfrak{R}e_i$. Then clearly, $\alpha_1, \dots, \alpha_m$ has e as right unit in \mathfrak{R} . If $\alpha_1, \dots, \alpha_m$ are all the elements of a set of matrices in $S_n(\mathfrak{R})$ then these matrices have for right unit the diagonal matrix with all diagonal elements equal to e , all other matrix elements equal to zero.

§ 4. Decomposition theorems for rings

Lemma 4.1. *Suppose \mathfrak{R} is left semi-regular. Then A, B have only 0 in common and hence $\alpha \rightarrow (\alpha + A, \alpha + B)$ is an isomorphic mapping of \mathfrak{R} onto a subring of the direct sum $\mathfrak{R}/B \oplus \mathfrak{R}/A$.*

Proof. If α is in both A and B then so is a left idempotent e of α since A and B are ideals, by Lemma 2.1. Then $ee=0$ so $e=0$, and $\alpha = \alpha e = 0$.

Lemma 4.2. *Suppose \mathfrak{R} is idempotent-associative and regular and every idempotent of \mathfrak{R} is in its centre. Then \mathfrak{R} contains a family of ideals N_λ such that each $\mathfrak{R}_\lambda = \mathfrak{R}/N_\lambda$ is idempotent-associative, regular and has a unit but no other non-zero idempotents and $\alpha \rightarrow (\alpha + N_\lambda)$ is an isomorphic mapping of \mathfrak{R} onto a subring of the direct sum of the N_λ .*

Proof. Let E denote the set of idempotents in \mathfrak{R} , ordered by: $e \leq f$ if $ef=e$. Then E is a Boolean ring. For each maximal ideal λ of E let N_λ denote the set of α in \mathfrak{R} for which $e\alpha = \alpha$ for some e in λ . Then N_λ is an ideal of \mathfrak{R} , since

(i) if α is in N_λ then $e\alpha = \alpha$ for some e in λ ; then $e(\alpha\beta) = \alpha\beta$, $e(\beta\alpha) = \beta(e\alpha) = \beta\alpha$ for this e ; thus $\alpha\beta, \beta\alpha$ are in N_λ for all β in \mathfrak{R} ;

(ii) if α, β are in N_λ then $e\alpha = \alpha, f\beta = \beta$ for some e, f in λ ; then, $e+f-ef$ is also in λ and, since e, f are commuting idempotents,

$$(e+f-ef)(\alpha+\beta) = (e+f-ef)(e\alpha+f\beta) = \alpha+\beta,$$

thus $\alpha+\beta$ is also in N_λ . Moreover, by the Corollary to Lemma 2.3, every idempotent in $\mathfrak{R}_\lambda = \mathfrak{R}/N_\lambda$ is of the form $e+N_\lambda$ with e idempotent in \mathfrak{R} .

Now let f be any idempotent not in λ . Then for every α in \mathfrak{R} , $\beta = \alpha - \alpha f$ satisfies $f\beta = 0$. Let e_1 be a left unit for β . Then $e = e_1 - e_1 f$ is also a left unit for β , i. e., $e\beta = \beta$. But $ef = 0$, hence the set $\bar{\lambda}$ consisting of

all $eh + g - ehg$ ($h \in E, g \in \lambda$) excludes f (and includes e). But $\bar{\lambda}$ is an ideal of E and $\bar{\lambda} \supseteq \lambda$. Hence $\bar{\lambda} = \lambda$ since λ is a maximal ideal of E . Thus λ contains e , hence (by definition) N_λ contains β . Now

$$\begin{aligned} (\alpha + N_\lambda)(f + N_\lambda) &= (f + N_\lambda)(\alpha + N_\lambda) = f\alpha + N_\lambda = \\ &= f\alpha + (\beta + N_\lambda) = (f\alpha + \beta) + N_\lambda = \alpha + N_\lambda \end{aligned}$$

showing that $f + N_\lambda$ is a unit of \mathfrak{R}_λ .

The mapping $\alpha \rightarrow (\alpha + N_\lambda)$ is an isomorphism. For, if $\alpha \neq 0$, then there exists an idempotent e with $\beta\alpha = e$, $\alpha e = \alpha$ (since \mathfrak{R} is regular) and, obviously, $e \neq 0$; hence there exists a maximal ideal λ in E for which $e \in \lambda$ is false (as is well known, such λ can be constructed with the help of ZORN's Lemma or by the usual transfinite induction); hence $\alpha \in N_\lambda$ is false. Thus $\alpha \rightarrow (N_\lambda)$ only if $\alpha = 0$.

Theorem 2. *Suppose \mathfrak{R} is idempotent-associative and regular. Then \mathfrak{R} is isomorphic to a subring of a direct sum $\bar{\mathfrak{R}} = \mathfrak{R}/B \oplus \Sigma \mathfrak{R}/N_\lambda$, where \mathfrak{R}/B is associative and regular and each \mathfrak{R}/N_λ is a regular ring with unit but no idempotents other than 0 and 1. \mathfrak{R} satisfies (\bar{P}_2) or (P_3) if and only if each \mathfrak{R}/N_λ satisfies (\bar{P}_2) , (P_3) respectively, and if only if each \mathfrak{R}/N_λ is a division ring without zero divisors or an alternative division ring, respectively.¹⁵⁾*

Proof. This follows from Lemma 4.1, Lemma 2.1, the Corollary to Lemma 2.4, Lemma 4.2 and Lemma 2.5, since \mathfrak{R} satisfies (\bar{P}_2) or (P_3) if and only if each homomorphic map \mathfrak{R}/N_λ satisfies (\bar{P}_2) or (P_3) respectively.

Corollary. *An idempotent-associative regular ring has property (P_3) if and only if it is alternative.*

§ 5. M -sets and S_n -matrices

\mathfrak{R} will denote a fixed ring, n a fixed integer ≥ 1 .

A vector $v = (\alpha^i; i = 1, \dots, n)$ with all α^i in \mathfrak{R} , will be called an r -vector (and we sometimes write $(\alpha^1, \dots, \alpha^r)$ for v) if $\alpha^i = 0$ for all $i > r$, a *controlled r -vector* if also α^r is idempotent ($= e(v) = e$, say) with $e\alpha^j = \alpha^j$ for all $j < r$.

A set of vectors v_1, \dots, v_n will be called a *basis* if each v_r is a controlled r -vector, *canonical* if also $\alpha_r^i e_i = 0$ for all $i < r$ where e_i denotes $e(v_i)$.

An M_n -set (or simply M -set), written $M(v_1, \dots, v_n)$, shall be defined whenever v_1, \dots, v_n is a basis and shall consist of all controlled vectors of

¹⁵⁾ Related decomposition theorems were given by FORSYTHE and MCCOY [4] and M. F. SMILEY [11].

the form $\gamma_1 v_1 + \dots + \gamma_n v_n$; v_1, \dots, v_n is called then a basis for $M(v_1, \dots, v_n)$. The set of all M -sets, ordered by inclusion, will be denoted $L^M = L_n^M = L_n^M(\mathfrak{R})$. We shall sometimes denote $M(v_1, \dots, v_n)$ by $[v_1, \dots, v_n]$ omitting some or all of those v_i which happen to be 0.

An S_n -matrix (or simply S -matrix) shall mean a matrix $X = (\alpha_i^r$; $r, i = 1, \dots, n)$ in $S = S_n(\mathfrak{R})$, i. e., the r -th row is an r -vector v_r with α_i^r associating. We sometimes write $\|v_1, \dots, v_n\|$ for X . The matrix X is called *canonical* if v_1, \dots, v_n is a canonical basis. If \mathfrak{R} is idempotent-associative then a canonical X is necessarily idempotent.

Lemma 5.1. *Suppose \mathfrak{R} is idempotent-associative. If $n = 1, 2$ or 3 then*

(i) $M(u_1, \dots, u_n) \subset M(v_1, \dots, v_n)$ if and only if all u_1, \dots, u_n are in $M(v_1, \dots, v_n)$,

(ii) every M -set has a canonical basis,

(iii) for every idempotent X in S there exists a canonical E in S with $XE = X$ and $EX = E$, (so that $SE = SX$, since S is an associative ring),

(iv) L^M and $L(S)$ are order-isomorphic under the correspondence $M \leftrightarrow SE$ if M consists of all controlled vectors occurring as rows in matrices of SE , where E is an idempotent in S .

Proof. We consider $n = 3$ only (the argument given will cover the cases $n = 1, 2$ also).

(i) can be verified easily by the reader.

(ii) If $(e_1), (\alpha, e_2), (\beta, \gamma, e_3)$ is a basis for the M -set then $(e_1), (\alpha - \alpha e_1, e_2), (\beta - \beta e_1 - \gamma(\alpha - \alpha e_1), \gamma - \gamma e_2, e_3)$ is a canonical basis for the M -set.

(iii) An idempotent X must have the form $\|(e), (\alpha, f), (\beta, \gamma, g)\|$ with e, f, g idempotent and $\alpha e + f\alpha = \alpha, \beta e + \gamma\alpha + g\beta = \beta, \gamma f + g\gamma = \gamma$. Now $E = \|(e), (f\alpha, f), (g\beta - g\beta e, g\gamma - g\gamma f, g)\|$ satisfies the requirements. This implies $SE = SEX \subseteq SX$ and $SX = SXE \subseteq SE$; i. e., $SE = SX$.

(iv) From (i), (ii) and (iii), L^M and $L(S)$ are order-isomorphic under the correspondence $M(u_1, u_2, u_3) \leftrightarrow \|u_1, u_2, u_3\|$ for canonical bases u_1, u_2, u_3 . Indeed, if u_1, u_2, u_3 and v_1, v_2, v_3 are each a canonical basis, then by (i) above, $M(u_1, u_2, u_3) \subset M(v_1, v_2, v_3)$ if and only if

$$u_1 = e_1 v_1, \quad u_2 = \alpha_{21} v_1 + e_2 v_2, \quad u_3 = \alpha_{31} v_1 + \alpha_{32} v_2 + e_3 v_3$$

for suitable α_{ij} and idempotents e_1, e_2, e_3 in \mathfrak{R} . But this condition is equivalent to

$$\|u_1, u_2, u_3\| = \|(e_1), (\alpha_{21}, e_2), (\alpha_{31}, \alpha_{32}, e_3)\| \|v_1, v_2, v_3\|$$

that is, to: $\|u_1, u_2, u_3\| \in S \|v_1, v_2, v_3\|$. From (ii) and (iii) it now follows that the correspondence given above is an order-isomorphism of all L^M and all $L(S)$.

Finally, suppose E is an idempotent in S , so that, by (iii), $SE = S\|u_1, u_2, u_3\|$ where u_1, u_2, u_3 is a canonical basis. If now w is a controlled vector in a matrix of SE , then w is a controlled vector of the form $\alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3$ and thus it is in $M(u_1, u_2, u_3)$. On the other hand, if w is a vector in $M(u_1, u_2, u_3)$ it must be a controlled vector of one of the forms

$$e_1 u, \quad \alpha_{21} u_1 + e_2 u_2, \quad \alpha_{31} u_1 + \alpha_{32} u_2 + e_3 u_3$$

and hence does occur as a row in a matrix obtained from $\|u_1, u_2, u_3\|$ by multiplying on the left by a matrix of one of the forms

$$\|(e_1), (0), (0)\|, \quad \|(0), (\alpha_{21}, e_2), (0)\|, \quad \|(0), (0), (\alpha_{31}, \alpha_{32}, e_3)\|.$$

This proves all parts of (iv).

Lemma 5.2. *Suppose \mathfrak{R} is idempotent-associative.*

(i) *If \mathfrak{R} is regular and e is a left idempotent for α , then $X = \|(0), (\alpha), (0)\|$ has $E = \|(e), (0), (0)\|$ for left idempotent in S_3 , and $\|(0), (\alpha)\|$ has $\|(e), (0)\|$ for left idempotent in S_2 , and every $X_1 = \|(0), (\alpha, \beta), (0)\|$ with β associating has a left idempotent $\|v_1, v_2, (0)\|$ in S_3 such that $\|(0), (\alpha, \beta)\|$ has $\|v_1, v_2\|$ as left idempotent in S_2 .*

(ii) *If (\bar{P}_2) holds in \mathfrak{R} , then every $X = \|(0), (0), (\alpha, \beta)\|$ has a left idempotent of the form $E = \|(e), (\gamma, f), (0)\|$ in S_3 , and every $X_1 = \|(0), (0), (\alpha, \beta, \gamma)\|$ with γ associating has a left idempotent in S_3 .*

Proof of (i). Clearly $XE = X$. If $F = \|u_1, \dots\|$ is idempotent (necessarily $u_1 = (h)$ with h idempotent) and $XF = X$ then $\alpha h = \alpha$. Hence $eh = e$ since e is a left idempotent for α . This implies $EF = E$ so E is a left idempotent for X .

Now, since β is associating, by Lemma 2.1 there is a left partial inverse $\beta' \in \mathfrak{R}^a$ for β . Then $E_1 = \|(0), (0, \beta' \beta \beta'), (0)\| X_1$ is canonical. By Lemma 3.1 and Corollary 2 to Theorem 1, X_1 has a left idempotent if $X_1 - X_1 E_1$ has a left idempotent, and this is so since $X_1 - X_1 E_1$ has the form $\|(0), (\alpha_1), (0)\|$.

Proof of (ii). By (\bar{P}_2) there exist idempotents e, f, g and an element δ such that $\beta f = \beta$ and for every $\eta, \beta \eta = 0$ implies $f \eta = 0$; $g \beta = \beta$ and $\beta \mathfrak{R} = g \mathfrak{R}$; $\delta(\alpha - g \alpha) = e$ and $(\alpha - g \alpha)e = \alpha - g \alpha$.

Then $\alpha - \alpha e = g \alpha - g \alpha e \in g \mathfrak{R} (= \beta \mathfrak{R})$, hence $\alpha - \alpha e = \beta \gamma$ for some γ . Since $\beta \gamma = (\beta f) \gamma = \beta (f \gamma)$, we may use $f \gamma$ as a new γ . After this change, we have $f \gamma = \gamma$. Since $\beta \gamma e = (\alpha - \alpha e)e = 0$ it follows that $f \gamma e = 0$, hence $\gamma e = 0$.

Now $E = \|(e), (\gamma, f), (0)\|$ is canonical, and $XE = X$. If $XF = X$ for any $F = \|(\theta), (\varrho, \varphi), u_3\|$ then $\alpha \theta + \beta \varrho = \alpha$, $\beta \varphi = \beta$ and θ, φ are associating.

To show E is a left idempotent for X we need only prove that $EF = E$, i. e., $e\theta = e$, $\gamma\theta + f\varrho = \gamma$, $f\varphi = f$. But, since $\alpha\theta = \alpha - \beta\varrho$ and $g\beta = \beta$,

$$e\theta = \delta(\alpha - g\alpha)\theta = \delta(\alpha - \beta\varrho - g(\alpha - \beta\varrho)) = \delta(\alpha - g\alpha) = e;$$

since $\alpha = \alpha e + \beta\gamma = \alpha\theta + \beta\varrho$ and $\beta f = \beta$,

$$\begin{aligned} \beta(\gamma\theta + f\varrho - \gamma) &= (\alpha - \alpha e)\theta + \beta\varrho - \beta\gamma = \alpha\theta - \alpha e + \beta\varrho - \beta\gamma = \\ &= (\alpha\theta + \beta\varrho) - (\alpha e + \beta\gamma) = 0, \end{aligned}$$

hence,

$$0 = f(\gamma\theta + f\varrho - \gamma) = \gamma\theta + f\varrho - \gamma \quad (\text{since } f\gamma = \gamma);$$

so $\gamma\theta + f\varrho = \gamma$. Finally, since $\beta = \beta f = \beta\varphi$, therefore $\beta(\varphi - f) = 0$, hence $f(\varphi - f) = 0$ so $f\varphi = f$. This completes the proof that E is a left idempotent for X .

Now if γ is associating, there is a left partial inverse $\gamma' \in \mathfrak{R}^a$ for γ . As in the proof of (i), X_1 has a left partial inverse since $E_1 = \|(0), (0), (0, 0, \gamma'\gamma\gamma)\|$ X_1 is canonical and $X_1 - X_1 E_1$ is of the form $\|(0), (0), (\alpha_1, \beta_1)\|$.

Theorem 3. *Suppose \mathfrak{R} is idempotent-associative.*

(i) *If \mathfrak{R} is regular then S_2 is semi-regular and L_2 is a relatively complemented modular lattice with zero, complemented with a homogeneous basis of order 2 if \mathfrak{R} has a right unit.*

(ii) *If (\overline{P}_2) holds then S_3 is semi-regular and L_3 is a relatively complemented modular lattice with zero, complemented with a homogeneous basis of order 3 if \mathfrak{R} has a right unit.*

Proof. We consider (ii) (the argument given will cover (i) also).

Proof of (ii): lattice character. We first show that every $X = \|(\alpha), (\beta, \gamma), (\lambda, \mu, \nu) \|$ in S_3 has a left idempotent.

Let e be a left unit for $\alpha, \beta, \gamma, \lambda, \mu, \nu$ (existing by Corollary 2 to Theorem 1; the Corollary applies since (\overline{P}_2) implies \mathfrak{R} is regular, a fortiori, semi-regular). Let $X_1 = \|(e), (0, e), (0)\|$ X . Now if X_1 has a left idempotent E , then Lemma 3.1 shows that X also has a left idempotent. Indeed, Lemma 3.1 applies with S_3 in place of \mathfrak{R} , X in place of α , and E in place of e ; (3.1) holds because for every idempotent G in S_3 , $X \in S_3 G$ implies $X = XG$, hence $X_1 G = X_1$ and so $EG = E$, that is, $E \in S_3 G$; further, $X - XE = \|(0), (0), (\lambda', \mu', \nu')\|$ has a left idempotent by Lemma 5.2 (ii). Thus we need consider only X_1 , i. e., we can suppose $\lambda = \mu = \nu = 0$. Similarly we can suppose $\beta = \gamma = 0$.

Now if $\alpha' \in \mathfrak{R}^a$ is a left partial inverse of α then $\|(\alpha'), (0), (0)\| \|(\alpha), (0), (0)\|$ is clearly a left idempotent for $\|(\alpha), (0), (0)\|$ in S_3 so that S_3 is left semi-regular.

By the dual argument,¹⁶⁾ S_3 is also right semi-regular, hence semi-regular. Then, by Theorem 1, L_3 is a relatively complemented lattice with zero.

Proof of (ii): modularity. By Theorem 2, \mathfrak{R} can be imbedded in a direct sur: $\overline{\mathfrak{R}} = \mathfrak{R}/B \oplus \Sigma \mathfrak{R}/N_\lambda$, and this induces a natural imbedding of $S_3(\mathfrak{R})$ in the direct sum $\overline{S}_3 = S_3(\mathfrak{R}/B) \oplus \Sigma S_3(\mathfrak{R}/N_\lambda)$. We have already shown that every X in $S_3(\mathfrak{R})$ has a left idempotent E in $S_3(\mathfrak{R})$ (for example, if $X = \|(\alpha), (0), (0)\|$ then $E = \|(\alpha'\alpha), (0), (0)\|$ where $\alpha' \in \mathfrak{R}^a$ is a left partial inverse of α ; but then this E is also a left idempotent for this X , considered in \overline{S}_3). Examination of Lemma 3.1 and Lemma 5.2 and their application to construct a left idempotent E in $S_3(\mathfrak{R})$ for arbitrary X in $S_3(\mathfrak{R})$ shows that E is also a left idempotent for X considered in \overline{S}_3 . A dual statement holds for right idempotents. So by Corollary 1 to Theorem 1, $L_3(\mathfrak{R}) = L(S_3(\mathfrak{R}))$ is lattice isomorphic to a sublattice of $L(\overline{S}_3) = L(S_3(\mathfrak{R}/B)) \oplus \Sigma L(S_3(\mathfrak{R}/N_\lambda))$. Thus, to prove L_3 modular we need only show that $L(S_3(\mathfrak{R}/B))$ is modular and that each $L(S_3(\mathfrak{R}/N_\lambda))$ is modular.

Since \mathfrak{R}/B is associative and regular, the work of VON NEUMANN [9], Part II, Proof of Theorem 2.13, shows¹⁷⁾ that $M_3(\mathfrak{R}/B)$ is associative and regular and that $L(M_3(\mathfrak{R}/B))$ is isomorphic to $L(S_3(\mathfrak{R}/B))$, so the latter is modular (for the definition of $M_n(\mathfrak{R})$ see § 1).

Thus, by Theorem 2, we need only show: $L_3(\mathfrak{R})$ is modular when \mathfrak{R} is a division ring with unit, and without zero divisors.

It is sufficient to show that $L_3^M(\mathfrak{R})$ is a projective plane geometry¹⁸⁾, hence modular. Clearly $M(u_1, u_2, u_3)$ is an atom if and only if exactly one

¹⁶⁾ The dual ring \mathfrak{R}' consists of the elements of \mathfrak{R} with addition unchanged but with multiplication $\alpha \circ \beta$ in \mathfrak{R}' coinciding with $\beta \alpha$ in \mathfrak{R} . Then $S_3(\mathfrak{R})$ is anti-isomorphic to $S_3(\mathfrak{R}')$ under the correspondence

$$\|(\alpha), (\beta, \gamma), (\lambda, \mu, \nu)\| \leftrightarrow \|(\nu), (\mu, \gamma), (\lambda, \beta, \alpha)\|.$$

Now the proof of left semi-regularity of $S_3(\mathfrak{R})$ is also a proof of left semi-regularity of $S_3(\mathfrak{R}')$ which is equivalent to right semi-regularity of $S_3(\mathfrak{R})$.

¹⁷⁾ J. VON NEUMANN showed that if \mathfrak{R} is regular and associative then $M_n(\mathfrak{R})$ is associative and regular for all $n = 1, 2, \dots$ so that for every A in $M_n(\mathfrak{R})$ there exists an idempotent E in $M_n(\mathfrak{R})$ with $M_n(\mathfrak{R})A = M_n(\mathfrak{R})E$. Now, although this is not stated explicitly, the argument given by VON NEUMANN actually shows that there exists such an E in $S_n(\mathfrak{R})$; hence, if \mathfrak{R} is associative and regular there is an obvious order-isomorphism between $L(M_n(\mathfrak{R}))$ and $L(S_n(\mathfrak{R}))$ for each $n = 1, 2, \dots$.

¹⁸⁾ We do not require \mathfrak{R} to be alternative, hence this plane projective geometry is more general than the geometry constructed by R. MOUFANG [8].

of the u_i is $\neq 0$ and $M(u_1, u_2, u_3)$ is the unit of L_3^M if all u_i are $\neq 0$; we shall call $M(u_1, u_2, u_3)$ a *line* if exactly two of the $u_i \neq 0$.

It is easily verified that if one line is contained in another, they are identical, it is obvious that every line contains at least two distinct points, and we know already (Lemma 5.1, (iv)) that L_3^M is a relatively complemented lattice. Therefore, to show that L_3^M is a projective plane we need only show:

- (i) two atoms are always contained in some line,
- (ii) two lines have at least one atom in common.

(i) is obvious except when the atoms are of the form $[(\alpha, \beta, 1)]$ and $[(\lambda, \mu, 1)]$. In this case, either $\beta = \mu$ and then both atoms are contained in the line $[(1), (\alpha, \beta, 1)]$; or $\beta \neq \mu$ and then both atoms are contained in the line $[(\gamma, 1), (\delta, 0, 1)]$ where δ is a solution for $(\mu - \beta)\delta = \lambda - \alpha$ and γ is the common value of $\lambda - \mu\delta = \alpha - \beta\delta$.

(ii) is obvious except when the lines are of the form $[(\alpha, 1), (\beta, 0, 1)]$ and $[(\lambda, 1), (\mu, 0, 1)]$ with $\alpha \neq \lambda$. Then $\gamma\alpha + \beta = \gamma\lambda + \mu$ for some γ ; with this γ , $[(\gamma\alpha + \beta, \gamma, 1)]$ is common to both lines.

This completes the proof of modularity of L_3 .

Proof of (ii): homogeneous basis. Finally, if \mathfrak{R} has a right unit e_0 , the following is readily verified to be a normalized frame for L_3^M : $a_1 = [(e_0)]$, $a_2 = [(0, e_0)]$, $a_3 = [(0, 0, e_0)]$, $c_{12} = c_{21} = [(-e_0, e_0)]$, $c_{13} = c_{31} = [(-e_0, 0, e_0)]$, $c_{23} = c_{32} = [(0, -e_0, e_0)]$.

Theorem 4. *Suppose \mathfrak{R} is an idempotent-associative, regular ring with unit for which (P_3) holds. Then*

(i) *every normalized frame of order 3 for L_3 satisfies the conditions (3.1.7), (5.1.1), (5.1.2) of [6],*

(ii) *the construction of [6], applied to the particular normalized frame given at the end of the proof of Theorem 3, yields a coordinatizing ring isomorphic to the original \mathfrak{R} , under the mapping $\alpha \leftrightarrow [(-\alpha, 0, 1)]$ ($\alpha \in \mathfrak{R}$, $[(-\alpha, 0, 1)] \in L_{31}$).*

(iii) *if \mathfrak{R} is the coordinatizing ring of some L' constructed as in [6], then L_3 is isomorphic to L' .*

Remark 1. We recall that if $a_1, a_2, a_3, c_{12} = c_{21}, c_{13} = c_{31}, c_{23} = c_{32}$ is a normalized frame for any complemented modular lattice L then L_{ij} denotes the set of x with $x \oplus a_j = a_i \oplus a_j$. If i, j, k are 1, 2, 3 in some order, then $P_{k:i}x$ denotes $(x + c_{ik})(a_i + a_j)$. In each L_{ij} , multiplication is defined by:

$$x \times y = (P_{k:i}x + P_{k:i}y)(a_i + a_j).$$

The conditions (5.1.1), (5.1.2) of [6] are equivalent to

$(M)_{ij}$: For all x, y in L_{ij} :

$$P_{k:j}(x \times y) = (P_{k:j}x) \times (P_{k:j}y),$$

$$P_{k:i}(x \times y) = (P_{k:i}x) \times (P_{k:i}y).$$

The condition (3.1.7) of [6] asserts

$(A)_{ij}$: For all x, y in L_{ij} , the value of $Z(x, y, p, q) = \{(x+p)(q+a_j) + (y+q)(p+a_j)\}(a_i+a_j)$ is independent of p, q provided that $p+q = a_i+q, q(a_i+a_j) = 0, pa_i \leq x$ and we write $x+y$ for the common value of $Z(x, y, p, q)$. Then $\alpha = (x_{ij}; i > j)$ is called an upper semi- L -number if for $i > j, x_{ij} \in L_{ij}$ and $P_{2:1}x_{31} = x_{32}, P_{2:3}x_{31} = x_{21}$. As shown in [6], the set of such α , under the operations $\alpha + \beta = (x_{ij} + y_{ij}), \alpha\beta = (x_{ij} \times y_{ij})$ for all $\alpha = (x_{ij}), \beta = (y_{ij})$ forms a ring \mathfrak{R} with unit having properties $(P_1), (P_2), (P_3)$ provided $(A)_{31}, (A)_{32}, (A)_{21}$ and $(M)_{31}$ all hold.

Remark 2. In an arbitrary ordered set

$a + b = c$ means: the union of a, b does exist and it is c ,

$ab = c$ means: the meet of a, b does exist and it is c .

Now consider $L_3(\mathfrak{R})$ where \mathfrak{R} is merely an idempotent-associative ring with unit (do not assume \mathfrak{R} to be regular). Then easy calculations show that $a_1 = [(1)], a_2 = [(0, 1)], a_3 = [(0, 0, 1)], c_{12} = c_{21} = [(-1, 1, 0)], c_{23} = c_{32} = [(0, -1, 1)], c_{13} = c_{31} = [(-1, 0, 1)]$ is a normalized frame, i. e., $a_1 + a_2 + a_3 = 1$ and $a_i \oplus a_j = c_{ij} \oplus a_k, a_i(a_j + a_k) = 0, c_{ij} = c_{ji}, (c_{ij} + c_{jk})(a_i + a_k) = c_{ik}$ for i, j, k all different. Moreover with respect to this frame, L_{31} consists precisely of all $[(-\alpha, 0, 1)]$ with arbitrary α in \mathfrak{R} and $P_{2:3}[(-\alpha, 0, 1)] = [(-\alpha, 1, 0)], P_{2:1}[(-\alpha, 0, 1)] = [(0, -\alpha, 1)]$. Finally if $x = [(-\alpha, 0, 1)]$ and $y = [(-\beta, 0, 1)]$, then

$$Z(x, y, c_{23}, a_2) = \{[(-\alpha, 1, 0)] + \{[(-\beta, 0, 1)] + [(0, 1)]\}([(1)] + [(-\alpha, 1, 0)])\}([(1)] + [(0, 0, 1)]) =$$

$$= \{[(-\alpha, 1, 0)] + [(-\beta, -1, 1)]\}([(1)] + [(0, 0, 1)]) =$$

$$= [(-(\alpha + \beta), 0, 1)],$$

$$x \times y = \{[(0, -\alpha, 1)] + [(-\beta, 1, 0)]\}([(1)] + [(0, 0, 1)]) =$$

$$= [(-\alpha\beta, 0, 1)].$$

Thus (ii) certainly holds if the construction of [6] is possible, i. e., if (i) holds (the above calculations are important in the problem of coordinatizing ordered sets much more general than those discussed in this paper, which are complemented modular lattices satisfying the special conditions enumerated in Remark 1 above).

Remark 3. If \mathfrak{R} is the coordinatizing ring of some L' as constructed in [6] then L_3^M is isomorphic to L' (as shown in [2], where L_3^M was called L_3).

Lemma 5.1 shows that the L_3 of the present paper is isomorphic to L_3^M so that (iii) is proved.

Proof of Theorem 4. We need only show (i), in view of Remarks 2, 3 above. Moreover, as in the proof of modularity in Theorem 3, we need prove (i) only for the two special cases: \mathfrak{R} is associative and regular or \mathfrak{R} is a division ring without zero divisors, with unit, in which (P_3) holds. Since the first case was settled by the work of VON NEUMANN [6], §§ 4.3, 4.8 we need only consider the second special case (L_3 is then a plane projective geometry).¹⁹⁾

As shown in [6], the conditions (3.1.7), (5.1.1), (5.1.2) of [6], i. e., $(A)_{ij}$ and $(M)_{ij}$ for all $i \neq j$, for an arbitrary normalized frame of order 3 in any projective plane geometry, follow from the following quadrangle condition (Q_6) , given in [6], § 6²⁰⁾.

(Q_6) : Suppose two quadrangles P_i and P'_i ($i = 1, 2, 3, 4$) and a line W are such that:

- (i) no three of the vertices of the same quadrangle lie on a common line;
- (ii) W contains none of the vertices of either quadrangle. For $i, j = 1, 2, 3, 4, i \neq j$, let $P_{ij} = (P_i + P_j)W$ and $P'_{ij} = (P'_i + P'_j)W$ (P_{ij}, P'_{ij} are necessarily points).

Suppose also that:

- (iii) $P_{14} = P_{23}, P'_{14} = P'_{23}$;
- (iv) $P_{ij} = P'_{ij}$ except possibly for the pair $(i, j) = (3, 4)$. Then (iv) holds also for the pair $(i, j) = (3, 4)$.

Thus the proof of Theorem 4 is completed by (ii) of the following lemma.

Lemma 5.3. *Let $L_3(\mathfrak{R})$ be the plane projective geometry defined by a fixed division ring \mathfrak{R} with unit without zero divisors and satisfying (P_3) .*

¹⁹⁾ Under our present assumptions on \mathfrak{R} , it is easy to show that this geometry coincides with the plane geometry constructed by R. MOUFANG starting from an arbitrary alternative division ring \mathfrak{R} [8]. It was shown by MOUFANG that in this geometry her condition (D_9) holds, which implies the "uniqueness of harmonic conjugate point" condition; as shown in [6], § 6, this in turn implies the conditions (3.1.7), (5.1.1), (5.1.2) of [6] if the diagonal points of a complete quadrangle are non-collinear. Here we do not suppose such non-collinearity of diagonal points and we give a complete proof.

²⁰⁾ To prove $(A)_{ij}$, choose $P_1 = p, P_2 = q, P_3 = (p+x)(q+a_j), P_4 = (q+y)(p+a_j), W = a_i + a_j$ (we may suppose $x \neq a_i, y \neq a_j$); to prove $(M)_{ij}$, first choose $P_1 = x \times y, P_2 = P_{k:j}x, P_3 = x, P_4 = P_{k:j}(x \times y), P'_1 = y, P'_2 = c_{ik}, P'_3 = c_{ij}, P'_4 = P_{k:j}y, W = a_j + a_k$ (we may suppose $x \neq a_i, y \neq a_i, y \neq c_{ij}$) then choose $P_1 = x \times y, P_2 = P_{k:i}y, P_3 = y, P_4 = P_{k:i}(x \times y), P'_1 = x, P'_2 = c_{kj}, P'_3 = c_{ij}, P'_4 = P_{k:i}x, W = a_i + a_k$ (we may suppose $x \neq a_i, y \neq a_i, x \neq c_{ij}$).

(i) If P_i and P'_i ($i=1, 2, 3$) are points such that the three P_i do not lie on a line and the three P'_i do not lie on a line then there is a lattice automorphism of $L_3(\mathfrak{R})$ which maps each P'_i on P_i ²¹).

(ii) (Q_6) holds in $L_3(\mathfrak{R})$.

Proof of (i). Since the product of automorphisms is an automorphism, we may suppose $P_i = a_i$ ($i=1, 2, 3$) where a_i, c_{ij} are as in Theorem 3 and the Remark 2 following Theorem 4. It is clearly sufficient to show for each $j=1, 2, 3$: if $P'_i = P_i$ for all $i < j$ then there is an automorphism of L_3 which leaves P'_i fixed for $i < j$ and maps P'_j onto P_j .

Consider the following functions²²) which map point onto point:

1) For arbitrary fixed γ, δ :

$$\psi[(\alpha, \beta, 1)] = [(\alpha + \gamma, \beta + \delta, 1)]$$

$$\psi[(\alpha, 1)] = [(\alpha, 1)]$$

$$\psi[(1)] = [(1)]$$

2)

$$\psi_{12}[(\alpha, \beta, 1)] = [(\beta, \alpha, 1)]$$

$$\psi_{12}[(\alpha, 1)] = [(\alpha^{-1}, 1)] \quad \text{if } \alpha \neq 0^{23}$$

$$\psi_{12}[(0, 1)] = [(1)]$$

$$\psi_{12}[(1)] = [(0, 1)]$$

3)

$$\psi_{23}[(\alpha, \beta, 1)] = [(\beta^{-1}\alpha, \beta^{-1}, 1)] \quad \text{if } \beta \neq 0$$

$$\psi_{23}[(\alpha, 0, 1)] = [(\alpha, 1)]$$

$$\psi_{23}[(\alpha, 1)] = [(\alpha, 0, 1)]$$

$$\psi_{23}[(1)] = [(1)].$$

The reader can verify easily that if u_1, u_2, u_3 is a canonical basis, then each of 1), 2), 3) maps $M(u_1, u_2, u_3)$ onto $M(v_1, v_2, v_3)$ where $[v_i]$ is the map of $[u_i]$, and hence each of 1), 2), 3) determines an automorphism. The reader can also verify that a suitable product of automorphisms of types 1), 2), 3) satisfies the requirements of (i).

Remark. From the work of BRUCK and KLEINFELD ([3] and [7]) it follows that for each fixed $\delta \neq 0$, there exists a function $\varphi(\alpha)$ which maps \mathfrak{R} onto itself and has the properties (see [10], page 196): for all α, β in \mathfrak{R} ,

$$\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$$

$$\varphi(\alpha\beta) = \varphi(\alpha)(\delta^\alpha \varphi(\beta))$$

²¹) If use is made of the work of BRUCK and KLEINFELD [3] and [7] it can be shown that four points P'_i , no three on a line, can be mapped onto four points P_i , no three on a line (see the Remark following the proof of (i)).

²²) See [8], p. 215.

²³) If $\beta \neq 0$, β^{-1} denotes the unique solution of $\beta^{-1}\beta = \beta\beta^{-1} = 1$.

(necessarily, $\varphi(1) = \delta^{-1}$, $\varphi(-1) = -\delta^{-1}$). Then a lattice automorphism is determined by the point function:

$$\begin{aligned} 4) \quad & \varphi[(\alpha, \beta, 1)] = [(\varphi(\alpha), \varphi(\beta), 1)] \\ & \varphi[(\alpha, 1)] = [(\delta\varphi(\alpha), 1)] \\ & \varphi[(1)] = [(1)]. \end{aligned}$$

With the use of 4), (i) can be sharpened as described in footnote 21. However, we do not make use of 4) and our proof of (ii) below can be read without knowledge of the Bruck—Kleinfeld structure theory.

Proof of (ii). Because of (i) we may now suppose that $P_{12} = P'_{12} = a_3 = [(0, 0, 1)]$ and $P_{23} = P_{14} = P'_{23} = P'_{14} = a_1 = [(1, 0, 0)]$; then $P_{13} = P'_{13} = [(\alpha, 0, 1)]$ for some α and $P_{24} = P'_{24} = [(\beta, 0, 1)]$ for some β . We shall calculate P_{34} and P'_{34} .

Clearly not both of P_1, P_2 are on $a_1 + a_2$ since P_3 is on $P_2 + a_1$. We may therefore suppose P_2 is not on $a_1 + a_2$ since we can always interchange the pairs P_1, P_4 and P_3, P_5 . Hence P_2 has the form $[(\gamma, \delta, 1)]$ with $\delta \neq 0$.

The possibilities for P_1 are:

$$[(\delta^{-1}\gamma, 1)] \text{ or } [(\theta(\delta^{-1}\gamma), \theta, 1)] \text{ with } \theta \neq 0;$$

we consider these two cases separately.

If $P_1 = [(\delta^{-1}\gamma, 1)]$ then P_3 must be $[(\alpha + \gamma, \delta, 1)]$, $P_4 = [(\delta^{-1}(\gamma - \beta), 1)]$, and $P_{34} = [(\alpha + \beta, 0, 1)]$.

If $P_1 = [(\theta(\delta^{-1}\gamma), \theta, 1)]$, P_3 must be $[(\alpha + \gamma - \delta(\theta^{-1}\alpha), \delta, 1)]$, $P_4 = [(\beta + \theta(\delta^{-1}\gamma - \delta^{-1}\beta), \theta, 1)]$ and $P_{34} = [(\varepsilon, 0, 1)]$ where

$$\varepsilon = \beta + \theta(\delta^{-1}\gamma - \delta^{-1}\beta) - \theta\{(\delta - \theta)^{-1}(-\beta - \theta(\delta^{-1}\gamma - \delta^{-1}\beta) + \alpha + \gamma - \delta(\theta^{-1}\alpha))\}.$$

To calculate ε we note that for all ρ :

$$(\delta - \theta)^{-1}(\theta\rho) = (\delta - \theta)^{-1}(\delta\rho - (\delta - \theta)\rho) = (\delta - \theta)^{-1}(\delta\rho) - \rho.$$

If $\rho = \delta^{-1}\gamma - \delta^{-1}\beta$, the above expression is equal to $(\delta - \theta)^{-1}(\gamma - \beta) - (\delta^{-1}\gamma - \delta^{-1}\beta)$. Hence

$$\begin{aligned} \varepsilon &= \beta + \theta(\delta^{-1}\gamma - \delta^{-1}\beta) + \theta((\delta - \theta)^{-1}(\gamma - \beta) - \\ & \quad - (\delta^{-1}\gamma - \delta^{-1}\beta)) - \theta((\delta - \theta)^{-1}(\alpha + \gamma - \beta - \delta(\theta^{-1}\alpha))) = \\ &= \beta + \theta\{(\delta - \theta)^{-1}(\gamma - \beta - \alpha - \gamma + \beta + \delta(\theta^{-1}\alpha))\} = \\ &= \beta + \theta\{(\delta - \theta)^{-1}(\delta(\theta^{-1}\alpha) - \alpha)\} = \\ &= \beta + \theta\{(\delta - \theta)^{-1}(((\delta - \theta) + \theta)(\theta^{-1}\alpha) - \alpha)\} = \\ &= \beta + \theta\{\theta^{-1}\alpha + (\delta - \theta)^{-1}(\alpha - \alpha)\} = \\ &= \beta + \theta(\theta^{-1}\alpha) = \alpha + \beta. \end{aligned}$$

Thus in all cases $P_{34} = [(\alpha + \beta, 0, 1)]$ so that, by the same calculation $P'_{34} = P_{34}$, as required to establish (ii). This completes the proof of (ii) and so Theorem 4 is completely proved.

Remark. Let P_1, P_2, P_3, P_4 be four points, no three of which lie on a line. Let

$$D_1 = (P_4 + P_1)(P_2 + P_3), D_2 = (P_4 + P_2)(P_1 + P_3), D_3 = (P_4 + P_3)(P_1 + P_2).$$

Then the diagonal points D_1, D_2, D_3 always lie on a line or never lie on a line according as $1 + 1 = 0$ or $1 + 1 \neq 0$ in \mathfrak{R} .

For, by Lemma 5.3 (i), we may suppose $P_1 = a_1, P_2 = a_2, P_3 = a_3$. Then $D_3 = [(\alpha, 0, 1)]$ for some $\alpha \neq 0$, and

$$[(\alpha + \alpha, 0, 1)] = ((D_1 + D_2)(P_1 + P_2) + P_4)(P_1 + P_3).$$

Thus $\alpha + \alpha = 0$ if and only if this last point is P_3 , i. e., if and only if $P_4 + (D_1 + D_2)(P_1 + P_2)$ contains P_3 ; since $P_4 + D_3$ contains P_3 , this means, if and only if $(D_1 + D_2)(P_1 + P_2)$ coincides with D_3 , or equivalently $D_1 + D_2$ contains D_3 . Thus D_1, D_2, D_3 lie on a line if and only if $\alpha + \alpha = 0$. But $\alpha + \alpha = \alpha(1 + 1)$; since $\alpha \neq 0$, $\alpha + \alpha = 0$ is equivalent to $1 + 1 = 0$.

Note (added in proof, August 14, 1959). P. JORDAN and H. FREUDENTHAL (see the references listed in our [10] as 103, 75 and 76) have constructed a lattice which is isomorphic to our $L_3(\mathfrak{R})$ for the case that \mathfrak{R} is the alternative division ring of Cayley numbers (octaves); they made use of the available conjugation $\alpha \rightarrow \bar{\alpha}$ in \mathfrak{R} and used Hermitian symmetric 3×3 matrices over \mathfrak{R} . This method of construction has been recently generalized to a general alternative division ring by T. SPRINGER (announced at the Freudenthal symposium, Utrecht, August, 1959).

References

- [1] ICHIRO AMEMIYA, On the representation of complemented modular lattices, *Journal Math. Soc. Japan*, 9 (1957), 263—279.
- [2] ICHIRO AMEMIYA and ISRAEL HALPERIN, Coordinatization of complemented modular lattices, *Proceedings Amsterdam*, 62 (1959), 70—78.
- [3] R. H. BRUCK and E. KLEINFELD, The structure of alternative division rings, *Proceedings American Math. Soc.*, 2 (1951), 878—890.
- [4] ALEXANDRA FORSYTHE and N. H. MCCOY, On the commutativity of certain rings, *Bulletin American Math. Soc.*, 52 (1946), 523—526.
- [5] K. D. FRYER and ISRAEL HALPERIN, The von Neumann coordinatization theorem for complemented modular lattices, *Acta Sci. Math.*, 17 (1956), 203—249.
- [6] K. D. FRYER and ISRAEL HALPERIN, On the construction of coordinates for non-Desarguesian complemented modular lattices. I, II, *Proceedings Amsterdam*, 61 (1958), 142—161.

- [7] E. KLEINFELD, Alternative division rings of characteristic 2, *Proceedings National Academy of Sciences USA*, 37 (1951), 818—820.
- [8] R. MOUFANG, Alternativkörper und der Satz vom vollständigen Vierseit (D_0), *Abhandlungen aus dem Math. Seminar der Hamburgischen Universität*, 9 (1933), 107—222.
- [9] J. VON NEUMANN, *Continuous Geometry*. Parts I, II, III (planographed lecture notes, Institute for Advanced Study, Princeton, 1936), to be published in book form by Princeton University Press in 1959.
- [10] G. PICKERT, *Projektive Ebenen* (Berlin, 1955).
- [11] M. F. SMILEY, Alternative regular rings without nilpotent elements, *Bulletin American Math. Soc.*, 53 (1947), 775—778.
- [12] M. ZORN, Theorie der alternativen Ringe, *Abhandlungen aus dem Math. Seminar der Hamburgischen Universität*, 8 (1930 - 31), 123—147.

QUEEN'S UNIVERSITY, CANADA,
TOKYO COLLEGE OF SCIENCE, JAPAN.

(Received January 6, 1959)