SOME REMARKS ON p-RINGS AND THEIR BOOLEAN GEOMETRY

JOSEPH L. ZEMMER

Introduction. In this paper the word *ring* will always mean a ring with identity, and the Boolean algebra associated with a Boolean ring B will mean the Boolean algebra corresponding to B in the one-to-one correspondence, described by Stone [10], between the set of all Boolean rings and the set of all Boolean algebras. In a Boolean algebra, $\cap$, $\cup$, $'$, will denote the operations of intersection, union, and complementation respectively.

A commutative ring R will be called a *Boolean valued ring* if there exists a Boolean algebra $\mathfrak{B}$, and a single valued mapping $x \rightarrow \phi(x)$ of R into $\mathfrak{B}$ satisfying:

(i) $\phi(x)=0$ if and only if $x=0$,

(ii) $\phi(xy)=\phi(x) \cap \phi(y)$,

(iii) $\phi(x+y) \subseteqq \phi(x) \cup \phi(y)$.

When such a mapping exists it will be called a *valuation* for R. It is not difficult to show that a ring is a Boolean valued ring if and only if it is isomorphic to a subdirect sum of integral domains. Hence every commutative regular ring is Boolean valued.

In a Boolean valued ring the function $d(x, y)=\phi(x-y)$ satisfies the usual requirements for a distance function, except that the "distance" is an element of a Boolean algebra. The investigation of the geometric properties of a Boolean ring with respect to the distance function defined above was begun by Ellis [3, 4] and has been extended by Blumenthal [1]. The present paper is mainly concerned with extending some of these results to a larger class of Boolean valued rings, namely the p-rings.

It seems that p-rings were first defined and studied by McCoy and Montgomery [7] in order to generalize the well known theorem of Stone on the structure of Boolean rings. In [7] it is shown that every p-ring is a subdirect sum of fields I_p. In any commutative ring R the idempotents form a Boolean ring with respect to the multiplication of

Received April 25, 1954, and in revised form Nov. 15, 1954. Presented to the American Mathematical Society, April 30, 1954. Most of the work contained in this paper was made possible by a University of Missouri Summer Research Fellowship held by the author in 1953. The author wishes to express his appreciation to the referee for making several substantial improvements, and to L. M. Blumenthal for many hours of stimulating conversation in connection with the paper.

R and addition defined by $x \oplus y = x + y - 2xy$ (see [6, Exercise 2, p. 211]). This Boolean ring will be called the Boolean ring of idempotents of R.

1. A representation theorem for p-rings. The main theorem of this section, Theorem 1, and its first corollary are due to Foster [5]. (This fact was unknown to the author until after this paper was presented to the Society.) The proof given here is different from Foster's and quite a bit shorter. Corollary 2 is, to the best of the author's knowledge, new. In connection with Corollary 2 reference is made to Stone's theorem [11, p. 383] on the automorphism group of a Boolean ring. It may be of some interest to note that it is a consequence of Theorem 1 that every p-ring is uniquely determined by the prime p and the Boolean ring of idempotents.

THEOREM 1. *Let B be a Boolean ring, p a fixed prime, R^* the set of all $(p-1)$-tuples of pairwise orthogonal elements of B. If addition and multiplication for elements of R^* are defined by*

$$\text{(i)} \qquad (a_1, a_2, \cdots, a_{p-1}) + (b_1, b_2, \cdots, b_{p-1}) = (c_1, c_2, \cdots, c_{p-1}) ,$$

where

$$c_i = \sum_{j=0}^{p-1} a_j b_{i-j}, \qquad a_0 = 1 + \sum_{j=1}^{p-1} a_j, \qquad b_0 = 1 + \sum_{j=1}^{p-1} b_j ,$$

and the integers i and j are reduced mod p; *and*

$$\text{(ii)} \qquad (a_1, a_2, \cdots, a_{p-1})(b_1, b_2, \cdots, b_{p-1}) = (d_1, d_2, \cdots, d_{p-1}) ,$$

where $d_i = \sum_{j=1}^{p-1} a_j b_{j^{-1}i}$, and j^{-1} is the least integer mod p *satisfying $jx \equiv 1$* mod p, *then R^* is a p-ring which has for its Boolean ring of idempotents a ring isomorphic to B. Further, every p-ring is isomorphic to a p-ring of this type.*

COROLLARY 1. *Every element a in a p-ring may be uniquely expressed in the form $a = a_1 + 2a_2 + \cdots + (p-1)a_{p-1}$, where $2, \cdots, p-1$ are the successive summands of 1 and the a_i are pairwise orthogonal idempotents.*

COROLLARY 2. *The automorphism group of a p-ring is isomorphic to the automorphism group of its Boolean ring of idempotents.*

Proof. The given Boolean ring B may be regarded as a subring of the ring of all functions defined on a set Ω with values in the two element field I_2. For a given prime p consider the ring A_p of all functions defined on Ω with values in the prime field I_p. Note that an idempotent

f in A_p takes on only the values 0 or 1 at each point of Ω. If there is an element g in B such that $g(\omega)=0$ if and only if $f(\omega)=0$, then f will be said to *belong to* B. Denote by $1, 2, \cdots, p-1$ the identity of A_p and its successive summands and define a subset $\bar{R}^*$ of A_p to be the set of all x for which the idempotents

$$x_i=1-(x-i)^{p-1}, \qquad i=1, 2, \cdots, p-1,$$

belong to B. Note that if $x \in \bar{R}^*$ then $x_0=1-\sum_{i=1}^{p-1} x_i$ is an idempotent and *belongs to* B. It is now easy to verify that

(i) $\bar{R}^*$ is a subring of A_p,

(ii) there is a one-to-one correspondence between $\bar{R}^*$ and the set R^* which preserves the operations, and

(iii) the Boolean ring of idempotents of $\bar{R}^*$ is isomorphic to B.

This takes care of the first part of the theorem.

Now, let R be a p-ring and B its Boolean ring of idempotents. The ring R may be regarded as a subring of the ring of all functions defined on a set Ω with values in I_p, and B as a subring of the ring of all functions defined on the same set Ω with values in I_2. Note that for each x in R, $1-(x-i)^{p-1}$ is an idempotent for $i=1, 2, \cdots, p-1$, and hence is an element of B (it should be pointed out that here the elements of B are a subset of R). Further, note that $x_i=1-(x-i)^{p-1}$ may be characterized as that function for which $x_i(\omega)=1$ if $x(\omega)=i$ and $x_i(\omega)=0$ if $x(\omega)\neq i$. It follows readily from this observation that the p-ring $\bar{R}^*$ constructed with B as in the first part of the theorem is precisely the given p-ring R.

The proof of Corollary 1 also follows readily from the observation made above. To prove Corollary 2 let R be a p-ring and B its Boolean ring of idempotents. Denote by $\mathfrak{A}_R$ and $\mathfrak{A}_B$ the automorphism groups of R and B respectively. Clearly, every T in $\mathfrak{A}_R$ is a permutation of the elements of B. Further,

$$(a \oplus b)T=(a+b-2ab)T=aT+bT-2TaTbT=aT+bT-2aTbT$$
$$=aT \oplus bT$$

for every $a, b \in B$, so that $T \in \mathfrak{A}_R$ determines an element T' in $\mathfrak{A}_B$. It is easily seen that the mapping $T \to T'$ of $\mathfrak{A}_R$ into $\mathfrak{A}_B$ is a homomorphism. It remains to show that the mapping is an isomorphic mapping of $\mathfrak{A}_R$ onto $\mathfrak{A}_B$. By Corollary 2, every a in R may be written

$$a=a_1+2a_2+\cdots+(p-1)a_{p-1},$$

where $a_i = 1-(a-i)^{p-1} \in B$. For each T' in $\mathfrak{A}_B$, define a mapping T of R into R by

$$aT = a_1T' + 2(a_2T') + \cdots + (p-1)(a_{p-1}T') .$$

Since T' has an inverse it follows that T also has an inverse, and hence that T is a one-to-one mapping of R onto R. Further, if $b \in R$, so that $b = b_1 + 2b_2 + \cdots + (p-1)b_{p-1}$, where $b_i \in B$, then by the theorem

$$a+b = c_1 + 2c_2 + \cdots + (p-1)c_{p-1} ,$$

where

$$c_i = a_0b_i \oplus a_1b_{i-1} \oplus \cdots \oplus a_{p-1}b_{i-(p-1)} .$$

Clearly,

$$c_iT' = a_0T'b_iT' \oplus a_1T'b_{i-1}T' \oplus \cdots \oplus a_{p-1}T'b_{i-(p-1)}T' .$$

Hence,

$$(a+b)T = c_1T' + 2(c_2T') + \cdots + (p-1)(c_{p-1}T') = aT + bT .$$

Similarly it is seen that $(ab)T = (aT)(bT)$ for all a, b in R. Thus, T is an automorphism of R. It follows from the definition of T that $aT = aT'$ in case a is an idempotent in R, and hence that the mapping $T \rightarrow T'$ defined above is a mapping of $\mathfrak{A}_R$ onto $\mathfrak{A}_B$. Finally, let $T \in \mathfrak{A}_R$ such that $T \rightarrow E'$, the identity of $\mathfrak{A}_B$. Then T is an automorphism of R which maps every idempotent into itself. If $a \in R$, so that $a = a_1 + 2a_2 + \cdots + (p-1)a_{p-1}$, then

$$aT = a_1T + 2(a_2T) + \cdots + (p-1)(a_{p-1}T) = a_1 + 2a_2 + \cdots + (p-1)a_{p-1} = a .$$

Thus, the kernel of the homomorphic mapping defined above contains only the identity of $\mathfrak{A}_R$, and hence $\mathfrak{A}_R$ and $\mathfrak{A}_B$ are isomorphic.

If B is the Boolean ring of idempotents of a p-ring R and $\mathfrak{B}$ the associated Boolean algebra, then the mapping $a \rightarrow \phi(a) = a^{p-1}$ of R onto $\mathfrak{B}$ obviously satisfies Conditions (i) and (ii) of the definition of a Boolean valued ring. That Condition (iii) is also satisfied is seen by verifying

$$(x+y)^{p-1} \subseteqq x^{p-1} + y^{p-1} - x^{p-1}y^{p-1}$$

for all x, y in R, where the addition and multiplication are those of R and the inclusion that of $\mathfrak{B}$. This relation is equivalent to the identity

$$(x+y)^{p-1}(x^{p-1} + y^{p-1} - x^{p-1}y^{p-1}) = (x+y)^{p-1} ,$$

which is readily verified (as pointed out by the referee) by noting that

$$z = x^{p-1} + y^{p-1} - x^{p-1}y^{p-1}$$

is the identity element for the subring of R generated by x and y, so that $(x+y)^t z=(x+y)^t$ for any positive integer t. It follows readily from the proof of Theorem 1 that

$$a^{p-1}=a_1+a_2+\cdots+a_{p-1},$$

where $a_i=1-(a-i)^{p-1}$. This completes the proof of the following.

THEOREM 2. *The mapping*

$$x\rightarrow\phi(x)=x^{p-1}=\sum_{i=1}^{p-1}[1-(a-i)^{p-1}]$$

of a p-ring R onto its Boolean algebra $\mathfrak{B}$ of idempotents is a valuation for R.

It may be of interest to mention that the principal ideals of a p-ring R form a Boolean algebra with respect to ideal union and intersection. This is a special case of a result of von Neumann [9] which states that the principal ideals of any commutative regular ring form a Boolean algebra. Further, it may be shown that the mapping $(x)\rightarrow x^{p-1}$ of the set of principal ideals of R onto its Boolean algebra of idempotents is an isomorphism. A proof of this may be obtained from the following two facts, (i) if x^{p-1} and y^{p-1} are any two idempotents in R then

$$z=x^{p-1}+y^{p-1}-x^{p-1}y^{p-1}$$

is their Boolean algebra union; and (ii) if (x) and (y) are any two principal ideals of R then (xy) and (z) are their intersection and union respectively.

2. The matrix ring B_{p-1}. It was mentioned in the introduction that a Boolean valued ring admits a distance function. This notion is made more precise by the following.

DEFINITION. An abstract set $\mathfrak{M}$ is called a *Boolean distance space* (or simply a Boolean space) if with each pair of elements a, b there is associated a unique element $d(a,b)$ of a Boolean algebra $\mathfrak{B}$ satisfying:

(i) $d(a, b)=d(b, a)$,

(ii) $d(a, b)=0$ if and only if $a=b$,

(iii) $d(a, b)\subseteqq d(a, c)\cup d(c, b)$ for all a, b, c in $\mathfrak{M}$.

It is readily verified that any Boolean valued ring becomes a Boolean space by defining $d(a, b)=\phi(b-a)$. It follows from Theorem 2 that every p-ring R is a Boolean space. Further, if in the representation of R by the elements of R^*, the elements of B in a particular $(p-1)$-tuple are thought of as "coordinates", then the sum of the coordinates is the distance between the given element and zero.

It is desirable at this point to consider a certain ring of matrices associated with a p-ring R. Let B be the Boolean ring of idempotents of R and denote by B_{p-1} the set of all $(p-1)\times(p-1)$ matrices with elements in B. Some of the matrices in B_{p-1} may be used to define transformations of R into itself as follows. Let $a \in R$ and a^* the element of R^* corresponding to a in the isomorphism of Theorem 1, let $M \in B_{p-1}$, and form the matrix product a^*M, using the addition $\oplus$ of the Boolean ring B. Clearly a^*M is a $(p-1)$-tuple of elements of B, but it may or may not be in R^*. If $a^*M \in R^*$, let b be the element of R corresponding to a^*M and write $b=aM$. If $x^*M \in R^*$ for all x in R, that is, xM is defined for all x in R, then M defines a transformation of R into itself. It is not difficult to see that a necessary and sufficient condition that a matrix $M=(a_{ij})$ in B_{p-1} define a transformation of R is that $a_{is}a_{it}=0$ for $i, s, t=1, 2, \cdots, p-1$, $s \neq t$, in other words, that each row of M be an element of R^*.

Before the next definition is given it should be recalled that for every matrix in the ring of $n \times n$ matrices over an arbitrary commutative ring, a determinant may be computed in the usual way. Further, it may be shown that such a matrix is nonsingular if and only if its determinant has an inverse in the given ring (see [6] or [8]). Thus, since in a Boolean ring the identity is the only element which has an inverse, M in B_{p-1} is nonsingular if and only if $\det(M)=1$.

DEFINITION. A nonsingular matrix $M=(a_{ij})$ in B_{p-1} for which

$$a_{is}a_{it}=0 , \qquad i, s, t=1, 2, \cdots, p-1, \ s \neq t,$$

is called *orthogonal* if $\phi(xM)=\phi(x)$ for all x in R.

It is readily verified that the set of orthogonal matrices in B_{p-1} is a subgroup of the group of nonsingular matrices. The next theorem will show that the set of orthogonal matrices coincides with the set of all nonsingular matrices for which $a_{is}a_{it}=0$, $s \neq t$, that is, all nonsingular matrices which define transformations of R. (The original version of Theorem 3 stated only that (i) and (iii) are equivalent. The author is indebted to the referee for pointing out that (ii) may be included, thus making possible a considerable simplification.)

THEOREM 3. *Let $M=(a_{ij}) \in B_{p-1}$ for which $a_{is}a_{it}=0$, $i, s, t=1, 2, \cdots, p-1$, $s \neq t$, then the following are equivalent:* (i) *M is orthogonal,* (ii) *M is nonsingular,* (iii) $MM'=I$.

Proof. That (i) implies (ii) is trivial. Suppose next that $M=(a_{ij})$ is any nonsingular matrix for which $a_{is}a_{it}=0$, $s\neq t$. Then M' is nonsingular, as is $M'M=(b_{jk})$. Note however that

$$b_{jk}=\sum_{i=1}^{p-1}a_{ij}a_{ik}=0$$

if $j\neq k$, so that $M'M$ is diagonal. Let the diagonal elements be $d_1, d_2, \cdots, d_{p-1}$, then since 1 is the only element of B which has an inverse, $\det(M'M)=d_1d_2\cdots d_{p-1}=1$, hence each $d_i=1$, or $M'M=I$. It follows that $M'=M^{-1}$, and hence $MM'=I$. Thus, (ii) implies (iii). Finally, let $M=(a_{ij})$ be a matrix with $a_{is}a_{it}=0$, $s\neq t$, and suppose that $MM'=I$. Then M is nonsingular and defines a transformation of R. Let $a\in R$, and let $(a_1, a_2, \cdots, a_{p-1})$ be the element of R^* corresponding to a in the isomorphism of Theorem 1, so that aM in R corresponds to the $(p-1)$-tuple $(b_1, b_2, \cdots, b_{p-1})$, where $b_i=\sum_{j=1}^{p-1}a_ja_{ji}$. By Theorem 2 and since $\sum_{i=1}^{p-1}a_{ji}=1$,

$$\phi(aM)=\sum_{i=1}^{p-1}b_i=\sum_{i=1}^{p-1}\left(\sum_{j=1}^{p-1}a_ja_{ji}\right)=\sum_{j=1}^{p-1}a_j\left(\sum_{i=1}^{p-1}a_{ji}\right)=\sum_{j=1}^{p-1}a_j=\phi(a)\ .$$

Thus M is orthogonal, (iii) implies (i) and this completes the proof of the theorem.

3. The group of motions of R. The group of orthogonal matrices in B_{p-1} will be used to describe the motions (isometries) of the Boolean space of a p-ring R. This is done in Theorem 4, which also contains (thanks to the referee) a geometric characterization of transformations $x\to xM$ of R defined by arbitrary matrices in B_{p-1}. First, two lemmas and a definition are needed. The lemmas are obvious and their proofs are omitted.

LEMMA 1. *In a Boolean algebra if $ax=0$ implies $ay=0$ then $y\subseteqq x$.*

LEMMA 2. *Let R be a p-ring, B its Boolean ring of idempotents, and B_{p-1} the matrix ring described in the last section. If $z\in B$, $a\in R$, and $M\in B_{p-1}$ such that xM is defined for all x in R then $z(aM)=(za)M$.*

DEFINITION. A one-to-one mapping $x\to f(x)$ of a Boolean space $\mathfrak{M}$ onto itself is called a *motion* (*isometry*) of $\mathfrak{M}$ if $d(f(x), f(y))=d(x, y)$ for all x, y in $\mathfrak{M}$.

THEOREM 4. *Let R, B, B_{p-1} be defined as in Lemma 2. The mapping $x\to f(x)$ of R into R has the properties*

(i) $f(0)=0$,

(ii) $d(f(x), f(y)) \subseteqq d(x, y)$,

if and only if there exists an $M=(a_{ij})$ *in* B_{p-1} *with* $a_{is}a_{it}=0$, $s \neq t$, *such that* $f(x)=xM$ *for all* x *in* R. *Further, the mapping is a motion if and only if* M *is orthogonal.*

COROLLARY. *The mapping* $x \rightarrow f(x)$ *of* R *into* R *satisfies* $d(f(x), f(y)) \subseteqq d(x, y)$ *if and only if* $f(x)=xM+a$ *for some* M *in* B_{p-1} *with* $a_{is}a_{it}=0$, $s \neq t$, *and* a *in* R. *Further, the mapping is a motion if and only if* M *is orthogonal.*

Proof. Let $M=(a_{ij}) \in B_{p-1}$ with $a_{is}a_{it}=0$, $s \neq t$, and consider the transformation $f(x)=xM$. That $f(0)=0$ is trivial. Let $a, b \in R$ and choose z in B so that $z \cdot \phi(b-a)=0$. Then $\phi(zb-za)=0$, hence $zb=za$ and $(zb)M=(za)M$. Thus, by Lemma 2,

$$z(bM-aM)=0 , \qquad z \cdot \phi(bM-aM)=0 ,$$

and hence by Lemma 1, $d(f(b), f(a)) \subseteqq d(b, a)$. Further, if M is orthogonal (recall that, by Theorem 3, orthogonality for such an M is equivalent to nonsingularity) and if y is chosen in B so that $y \cdot \phi(bM-aM)=0$ then by Lemma 2, $(yb)M=(ya)M$. Since M is nonsingular this implies $yb=ya$ and hence that $y \cdot \phi(b-a)=0$. Thus, $d(b, a) \subseteqq d(f(b), f(a))$ which, together with the other inequality, gives $d(f(b), f(a))=d(b, a)$. Since M has an inverse it follows that $x \rightarrow f(x)$ is a motion of the Boolean space of R.

Next, suppose that $x \rightarrow f(x)$ is a transformation of R with the properties (i) and (ii) stated in the theorem. Then $\phi(f(x)) \subseteqq \phi(x)$ for all x in R. Let $a_i=f(i)$, $i=1, 2, \cdots, p-1$, and let $(a_{i1}, a_{i2}, \cdots, a_{i,p-1})$ be the element in R^* corresponding to a_i in the isomorphism of Theorem 1. Define M in B_{p-1} to be the matrix whose ith row is $(a_{i1}, a_{i2}, \cdots, a_{i,p-1})$ and note that M defines a transformation of R. Now, let $x \in R$, then clearly

$$\phi(f(x)-xM) \subseteqq \phi(f(x)) \cup \phi(xM) \subseteqq \phi(x) .$$

Further,

$$\phi(f(x)-xM)$$
$$=\phi(f(x)-f(i)+iM-xM) \subseteqq \phi(f(x)-f(i)) \cup \phi(iM-xM) \subseteqq \phi(x-i) ,$$

for $i=1, 2, \cdots, p-1$. Hence

$$\phi(f(x)-xM) \subseteqq \prod_{k=0}^{p-1} \phi(x-k)=\phi\left[\prod_{k=0}^{p-1}(x-k)\right]=\phi(x^p-x)=0 ,$$

and hence $f(x)=xM$. If, in addition, $x \to f(x)$ is a motion, then, since $\phi(i)=1$, $i=1, 2, \cdots, p-1$, it follows that

$$\sum_{j=1}^{p-1} a_{ij}=\phi(a_i)=1 .$$

Let $z_{ijk}=a_{ik}a_{jk}$, $i, j, k=1, 2, \cdots, p-1$, $i \neq j$, and note that $z_{ijk}a_i=z_{ijk}a_j=kz_{ijk}$, whence $z_{ijk}(a_i-a_j)=0$. Since

$$\phi(a_i-a_j)=\phi(f(i)-f(j))=\phi(i-j)=1 ,$$

it follows that a_i-a_j has an inverse in R. Thus, $a_{ik}a_{jk}=z_{ijk}=0$, $i \neq j$, and hence $MM'=I$. By Theorem 3, M is orthogonal and this completes the proof of the theorem.

The corollary is obtained by an obvious application of the theorem.

In case $p=2$ it is clear that B_{p-1} contains only one orthogonal element. Thus, the corollary to Theorem 4 generalizes a result of Ellis [4] which states that any motion $x \to f(x)$ of the Boolean space of a Boolean ring may be written $f(x)=x+a$. This result can also be easily proved without reference to Theorem 4, thus, if R is a Boolean ring and $x \to f(x)$ a motion of the Boolean space of R then, since $d(x, y)=x-y$, $f(x)-f(y)=x-y$, and hence $f(x)=x+f(0)$.

4. Superposability. Two subsets $\mathfrak{A}$ and $\mathfrak{B}$ of a Boolean space $\mathfrak{M}$ are said to be *congruent* if there is a one-to-one mapping of $\mathfrak{A}$ onto $\mathfrak{B}$ which preserves distances. If the congruent mapping of $\mathfrak{A}$ onto $\mathfrak{B}$ may be extended to a motion of $\mathfrak{M}$, then $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *superposable*. In case every two congruent subsets of $\mathfrak{M}$ are superposable $\mathfrak{M}$ is said to have the property of *free mobility*. Ellis [3] has shown that the Boolean space of a Boolean ring has the property of free mobility. It will be shown in this section that this is in general not true for a p-ring with $p>2$. In fact the following theorem and its corollary will be proved.

THEOREM 5. *Let R be a p-ring, $p>2$, B its Boolean ring of idempotents and $\mathfrak{B}$ the Boolean algebra associated with B. A necessary and sufficient condition that the Boolean space of R have the property of free mobility is that $\mathfrak{B}$ be a complete Boolean algebra.*

COROLLARY. *Every two congruent, finite subsets of the Boolean space of a p-ring are superposable.*

The following two lemmas are needed in the proof of the theorem. It should be pointed out that the validity and proof of Lemma 4 are unchanged if the matrix ring B_{p-1} is replaced by the ring of $n\times n$ matrices over any Boolean ring.

LEMMA 3. *Let a, b be elements of a Boolean valued ring S. If $ab=0$ then*

$$\phi(a+b)=\phi(a)\cup\phi(b) .$$

Proof. By commutativity $ba=ab=0$, so that

$$\phi(a+b)[\phi(a)\cup\phi(b)]=\phi(a+b)\phi(a)\cup\phi(a+b)\phi(b)=\phi(a^2)\cup\phi(b^2)=\phi(a)\cup\phi(b) .$$

Hence, $\phi(a)\cup\phi(b)\subseteqq\phi(a+b)$. This last relation, together with $\phi(a+b)\subseteqq\phi(a)\cup\phi(b)$, implies $\phi(a+b)=\phi(a)\cup\phi(b)$.

LEMMA 4. *Let R, B, B_{p-1} be defined as in Lemma 2. If $M=(a_{ij})\in B_{p-1}$ for which $a_{ij}a_{kj}=0$ and $a_{ji}a_{jk}=0$, for $i,j,k=1,2,\cdots,p-1$, $i\neq k$, then there exists a matrix $C=(c_{ij})$ in B_{p-1} such that*

(i) *$M+C$ is orthogonal,*

(ii) *$c_{ir}c_{is}=0$, for $i,r,s=1,2,\cdots,p-1$, $r\neq s$,*

(iii) *$a_{ir}c_{is}=0$, for $i,r,s=1,2,\cdots,p-1$.*

Proof. (The following proof is due to the referee. It is much more simple and considerably shorter than the author's.) Suppose first that B is the field I_2 so that M is a matrix with at most a single 1 in each row and each column. Then the desired matrix C must satisfy (i) $M+C$ is nonsingular, (ii) C has at most a single 1 in each row, and (iii) C has a zero row if the corresponding row of M is not zero. It is not difficult to see that there exists a matrix C satisfying (ii) and (iii) and such that $M+C$ has exactly one 1 in each row and column. Next suppose that B is an arbitrary Boolean ring. Then the elements a_{ij} of M together with 1 generate a finite Boolean ring $B'\subseteqq B$. It is sufficient to find a matrix C with elements in B'. However, since B' is a complete direct sum of fields I_2, the desired matrix C may be obtained by applying the process above to each summand in the direct sum.

Proof of Theorem 5. Let R be a p-ring for which the Boolean algebra $\mathfrak{B}$ associated with the Boolean ring of idempotents is complete. Let S_1 and T_1 be any two subsets of R which are congruent under the mapping $x\rightarrow h_1(x)$ of S_1 onto T_1. For some a in S_1 consider the motions $x\rightarrow s(x)=x-a$, and $x\rightarrow t(x)=x-h_1(a)$. The subsets S_1 and T_1 are mapped by these motions into subsets $S=s(S_1)$ and $T=t(T_1)$ which are congruent under the mapping

$$x \to h(x) = h_1(x+a) - h_1(a) .$$

Clearly S and T both contain 0, and $h(0)=0$. It follows that $\phi(h(x))=\phi(x)$ for x in S. To facillitate the following discussion let $\bar{x}=h(x)$ for each x in S, and let $(x_1, x_2, \cdots, x_{p-1})$ and $(\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_{p-1})$ be the elements in R^* corresponding respectively to x and $\bar{x}$ in the isomorphism of Theorem 1. For each $i, j=1, 2, \cdots, p-1$ define $a_{ij}=\bigcup_{x\in S} x_i\bar{x}_j$, and let $M=(a_{ij})$. Note that even though a_{ij} is defined by an operation of $\mathfrak{B}$ it is nevertheless an element of B. For fixed i and $j\neq k$ and any y, z in S consider the product $b=(y_i\bar{y}_j)(z_i\bar{z}_k)$. Clearly, $by_i=b\bar{y}_j=bz_i=b\bar{z}_k=b$. Since the elements in any $(p-1)$-tuple in R^* are pairwise orthogonal, it follows that $by_s=by_iy_s=0$ for $s\neq i$. Similarly, $b\bar{y}_s=0$ for $s\neq j$, $bz_s=0$ for $s\neq i$, and $b\bar{z}_s=0$ for $s\neq k$. Hence,

$$by=b(y_1+2y_2+\cdots+(p-1)y_{p-1})=iby_i=ib .$$

Similarly, $bz=ib$, $b\bar{y}=jb$, and $b\bar{z}=kb$. Since $x\to\bar{x}$ is a congruent mapping of S onto T, $\phi(y-z)=\phi(\bar{y}-\bar{z})$, and since $j\neq k$, $\phi(j-k)=1$. Hence,

$$\begin{aligned} b&=b\cdot\phi(j-k)=\phi(jb-kb)=\phi(b\bar{y}-b\bar{z})=b\phi(\bar{y}-\bar{z})=b\phi(y-z)\\ &=\phi(by-bz)=\phi(ib-ib)=0 .\end{aligned}$$

Thus,

$$a_{ij}a_{ik}=(\bigcup_{y\in S} y_i\bar{y}_j)(\bigcup_{z\in S} z_i\bar{z}_k)=0$$

in $\mathfrak{B}$ and hence also in B. Similarly it may be shown that $a_{ij}a_{kj}=0$ for $i, j, k=1, 2, \cdots, p-1$, $i\neq k$. Thus, M satisfies the hypotheses of Lemma 4 and hence there exists a matrix C in B_{p-1} such that $M+C$ is orthogonal. The matrix $M+C$ defines a motion of R, and the matrix M defines, at least, a transformation of R into R, as described in § 2. The transformation defined by M maps S onto a subset S^*, which will now be examined. For s in S, let $s^*=sM$, and note that $a_{ij}\geqq s_i\bar{s}_j$ follows from the definition of a_{ij}. Thus, $s_ia_{ij}\geqq s_i\bar{s}_j$, and since for pairwise orthogonal elements x_i in $\mathfrak{B}$, $\bigcup x_i=\sum x_i$ in B, it follows that

$$s_j = \sum_{i=1}^{p-1} s_ia_{ij} \geqq \sum_{i=1}^{p-1} s_i\bar{s}_j=\phi(s)\bar{s}_j=\phi(\bar{s})\bar{s}_j=\bar{s}_j ,$$

or

$$s_j^* \geqq \bar{s}_j , \qquad j=1, 2, \cdots, p-1 . \tag{1}$$

Further,

$$\phi(s^*)=\sum_{j=1}^{p-1}\sum_{i=1}^{p-1} s_ia_{ij}=\sum_{i=1}^{p-1} s_i\left(\sum_{j=1}^{p-1} a_{ij}\right)\subseteq\sum_{i=1}^{p-1} s_i=\phi(s)=\phi(\bar{s}) ,$$

and from (1) it follows that $\phi(s^*) \supseteqq \phi(\bar{s})$. Thus,

$$\phi(s^*) = \phi(\bar{s}) \ . \tag{2}$$

If $r \neq j$, it follows from (1) that $s_r^* \bar{s}_j \subseteqq s_r^* s_j^* = 0$, and hence that $s_r^* \bar{s}_j = 0$. From (2),

$$\sum_{i=1}^{p-1} s_i^* = \sum_{i=1}^{p-1} \bar{s}_i \ ,$$

whence

$$s_j^* = s_j^* \sum_{i=1}^{p-1} s_i^* = s_j^* \sum_{i=1}^{p-1} \bar{s}_i = s_j^* \bar{s}_j \ .$$

It follows that $s_j^* \subseteqq \bar{s}_j$, and this together with (1) gives $s_j^* = \bar{s}_j$, hence $sM = s^* = \bar{s} = h(s)$. Thus, the transformation defined by M maps S onto T and coincides with the congruence $s \to h(s)$.

It remains to show that $sM = s(M+C)$ for s in S. By Lemma 4, $c_{ij} a_{ir} = 0$, $i, r, j = 1, 2, \cdots, p-1$. For s in S let $b = s_i c_{ij}$, then $b \cdot a_{ir} = 0$. Since

$$a_{ir} = \bigcup_{x \in S} x_i \bar{x}_r \supseteqq s_i \bar{s}_r \ ,$$

it follows that

$$0 = b a_{ir} \supseteqq b s_i \bar{s}_r = b \bar{s}_r \ ,$$

or that $b\bar{s}_r = 0$, $r = 1, 2, \cdots, p-1$. Thus, $b\phi(s) = b\phi(\bar{s}) = 0$, whence $bs_i = 0$. Consequently $s_i c_{ij} = b = bs_i = 0$ for $i, j = 1, 2, \cdots, p-1$. Thus, $s(M+C) = sM$ for s in S, and the motion of R defined by $M+C$ coincides with $h(s)$ on S. Finally, let α, β, γ be the motions of R defined by the mappings $x \to s(x) = x - a$, $x \to x(M+C)$, $x \to t(x) = x - h_1(a)$, respectively, and note that the motion $\alpha\beta\gamma^{-1}$ coincides on S_1 with the congruence $x \to h_1(x)$ of S_1 onto T_1.

To prove the necessity it will be shown that a p-ring, $p > 2$, whose Boolean algebra of idempotents is not complete does not have the property of free mobility. Let $\mathfrak{B}$ be a Boolean algebra which is not complete, and let X be a subset of $\mathfrak{B}$ for which no least upper bound exists. Since $x \subset 1$ for all x in X, the set X^* of all upper bounds to X is not vacuous. Let Y be the set of complements of elements of X^*. It will be shown that if x, y are any upper bounds to X, Y respectively then $xy \neq 0$. Suppose on the contrary that $xy = 0$, then since x is not a least upper bound to X, there exists a $z \subset x$ which is an upper bound to X. Then $z' \in Y$, hence $z' \subseteqq y$, and $xz' \subseteqq xy = 0$, or $xz' = 0$, whence $xz = x$. It follows that $x \subseteqq z \subset x$, a contradiction. Thus, $xy \neq 0$ as stated. Note, however, that for all a in X, b in Y, $ab = 0$.

Now, let R be a p-ring, $p>2$, with $\mathfrak{B}$ as its Boolean algebra of idempotents, and let X, Y be the subsets of $\mathfrak{B}$ described above. Suppose, without loss of generality, that the cardinality of Y is greater than or equal to the cardinality of X. Then there is a one-to-one correspondence between X and a subset Y_1 of Y, say $x \longleftrightarrow f(x)$. Denote by Y_2 the subset of Y consisting of those elements which are not in $f(X)$, and define subsets A and B of R as follows: A contains 0, each y in Y_2, and for each x in X, the element $x+f(x)$; B contains 0, $2y$ for each y in Y_2, and for each x in X, the element $x+2f(x)$. Consider the mapping $z \rightarrow F(z)$ of A onto B defined by

$$F(z)=\begin{cases} 0 & \text{if } z=0\,, \\ 2y & \text{if } z=y\,, \\ x+2f(x) & \text{if } z=x+f(x)\,, \end{cases}$$

To see that

$$\phi(F(z_1)-F(z_2))=\phi(z_1-z_2)\ ,$$

for all z_1, z_2 in A, note first that $\phi(F(z))=\phi(z)=z$ for all z in A, and hence that if either $z_1=0$ or $z_2=0$, the equality is immediate. Also, the equality is obvious if $z_1, z_2 \in Y_2 \subset A$. If $z_1=x_1+f(x_1)$ and $z_2=x_2+f(x_2)$ then

$$\phi(F(z_1)-F(z_2))=\phi[(x_1-x_2)+2(f(x_1)-f(x_2))]\ ,$$

and since $(x_1-x_2)(f(x_1)-f(x_2))=0$, it follows from Lemma 3 that

$$\phi(F(z_1)-F(z_2))=\phi(x_1-x_2)+\phi(f(x_1)-f(x_2))\ .$$

Similarly,

$$\phi(z_1-z_2)=\phi(x_1-x_2)+\phi(f(x_1)-f(x_2))\ .$$

Finally, if $z_1=x+f(x)$ and $z_2=y \in Y_2$, then, again by the use of Lemma 3,

$$\begin{aligned}\phi(F(z_1)-F(z_2))&=\phi[x+2(f(x)-y)]=\phi(x)+\phi(f(x)-y)\\ &=\phi(x+f(x)-y)=\phi(z_1-z_2)\ .\end{aligned}$$

Thus, $z \rightarrow F(z)$ is a congruent mapping of A onto B. Suppose that A and B are superposable. Then there exists an orthogonal matrix $M=(m_{ij})$ in B_{p-1} such that the motion $x \rightarrow xM$ coincides with $F(x)$ on A, or $F(x)=xM$ for all x in A. Thus,

$$(3)\qquad \begin{cases} \text{(i)}\quad x+2f(x)=[x+f(x)]M & \text{for } x \text{ in } X, \\ \text{(ii)}\qquad 2y=yM & \text{for } y \text{ in } Y_2\,. \end{cases}$$

It follows from (3) (i) that

$$x+2f(x)=[x+f(x)]m_{11}+[x+f(x)]m_{12} ,$$

or that

$$x=[x+f(x)]m_{11} , \qquad f(x)=[x+f(x)]m_{12} ,$$

whence $x=xm_{11}$, $f(x)=f(x)m_{12}$, so that

$$(4) \qquad \text{(i)} \quad x \subseteqq m_{11} , \qquad \text{(ii)} \quad f(x) \subseteqq m_{12} , \qquad \text{for all } x \text{ in } X.$$

Similarly, from (3) (ii) it follows that

$$(5) \qquad y \subseteqq m_{12} , \qquad \text{for all } y \text{ in } Y_2 .$$

Relations (4) and (5) state that m_{11} is an upper bound to X, and m_{12} an upper bound to Y. But $m_{11}m_{12}=0$, and this contradicts the choice of X and Y. Thus, the congruent subsets A and B of R are not superposable. This completes the proof of the theorem.

Proof of the corollary. If the congruent subsets S_1 and T_1 in the sufficiency part of the proof are finite then

$$a_{ij}=\bigcup_{x \in S} x_i \bar{x}_j$$

exists whether $\mathfrak{B}$ is complete or not. The sufficiency proof then shows that S_1 and T_1 are superposable.

5. Betweenness and linearity. Let R be a p-ring, B its Boolean ring of idempotents, and $\mathfrak{B}$ the Boolean algebra associated with B. Since $\phi(a-b)=a \oplus b$ for all a, b in B, it follows that the subset B of R is congruent to the autometrized Boolean algebra $\mathfrak{B}$ (autometrized Boolean algebra is the name given by Ellis [3] to what is here called the Boolean space of a Boolean ring (2-ring)). The same is true for the image of B under any motion of R. The subset $f(B)$, where f is any motion of R, will be called a *one-dimensional subspace* of R. Note that in view of Theorem 5 the set of all one-dimensional subspaces of R is not necessarily the same as the set of all subsets of R congruent to $\mathfrak{B}$, unless $\mathfrak{B}$ is a complete Boolean algebra. In any event, all of the results of Blumenthal [1] are applicable to a one-dimensional subspace of R. For example, one is led to define betweenness for elements of R as follows:

DEFINITION. Let $a, b, c \in R$, then b is said to be *between* a and c if and only if

(i) $a \neq b \neq c$,

(ii) a, b, c are contained in a one-dimensional subspace of R,

(iii) $\phi(b-a) \cup \phi(c-b) = \phi(c-a)$.

The symbol $\beta(a, b, c)$ will mean that b is between a and c.

Following Blumenthal [1] a set of m pairwise distinct elements of R is said to be a β-linear m-tuple provided there exists a labeling, a_1, $a_2, \cdots, a_m$ such that $\beta(a_{i_1}, a_{i_2}, a_{i_3})$ holds for all $1 \leqq i_1 < i_2 < i_3 \leqq m$.

The following theorem now follows almost immediately from the corresponding theorem for an autometrized Boolean algebra [1, Theorem 4.2, p. 9].

THEOREM 6. *If each triple of pairwise distinct elements of an m-tuple, $m > 4$, is β-linear then the m-tuple is β-linear.*

Proof. Since each triple is congruent to a subset of the autometrized Boolean algebra $\mathfrak{B}$, whose elements are the idempotents of R, it follows from a theorem of Ellis [3, Theorem 5.1, p. 92] that the m-tuple is congruent to an m-tuple of $\mathfrak{B}$, for which all triples are β-linear. Hence, by the theorem of Blumenthal referred to above, the given m-tuple is β-linear.

6. Two unsolved problems. A set of k elements, $a_1, a_2, \cdots, a_k$, of a Boolean space is called a *metric basis* for the space if x is the only point with distances $d(a_i, x)$ from the a_i. It is not difficult to show that in the Boolean space of a p-ring R the elements $1, 2, \cdots, p-1$ form a metric basis. However, necessary and sufficient conditions that a subset $A \subseteqq R$ form a metric basis are not known.

Another unsolved problem is the extension to the Boolean space of a p-ring, $p > 2$, of the result of Ellis used in the proof of Theorem 6. Ellis calls an abstract set Σ a *B-metrized space* if with each x, y in Σ there is associated an element $d(x, y)$ of a Boolean algebra $\mathfrak{B}$, satisfying: (i) $d(x, y) = 0$, if and only if $x = y$, and (ii) $d(x, y) = d(y, x)$ for all x, y in Σ. Thus, a Boolean space is a B-metrized space in which $d(x, z) \subseteqq d(x, y) \cup d(y, z)$ holds for all x, y, z. Ellis has shown in [3] that a given abstract B-metrized space Σ is congruent to a subset of the Boolean space of a Boolean ring R if every three points of Σ are congruent to some set of three points in R, and further, that three is the smallest integer for which this is true. Whether or not there exists such an integer in case R is a p-ring, $p > 2$, is not known. If such an integer n exists for a p-ring R, then n is called the best congruence order of the Boolean space of R with respect to the class of B-metrized spaces. The reader is referred to Blumenthal [2] for a discussion of congruence orders of Euclidean spaces, and the metric characterization problem.

REFERENCES

1. L. M. Blumenthal, *Boolean geometry* I, Rend. Circ. Mat. Palermo, Series 2, **1** (1952), 1–18.

2. ———, *Theory and applications of distance geometry*, The Clarendon Press. Oxford, 1953.

3. David Ellis, *Autometrized Boolean algebras* I, Canadian J. Math., **3** (1951), 87–93.

4. ———, *Autometrized Boolean algebras* II, Canadian J. Math., **3** (1951), 145–147.

5. A. L. Foster, *p-rings and their Boolean-vector representation*, Acta Math., **84** (1951), 231–261.

6. Nathan Jacobson, *Lectures in abstract algebra*, Vol. I, *Basic concepts*, van Nostrand, New York, 1951.

7. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean rings*, Duke Math. J., **3** (1937), 455–459.

8. N. H. McCoy, *Rings and ideals*, The Carus Mathematical Monographs, no. 8, The Mathematical Association of America, 1948.

9. John von Neumann, *On regular rings*, Proc. Nat. Acad. Sci. U.S.A., **22** (1936), 707–713.

10. M. H. Stone, *The theory of representations for Boolean algebras*, Trans. Amer. Math. Soc., **40** (1936), 37–111.

11. ———, *Applications of the theory of Boolean rings to general topology*, Trans. Amer. Math. Soc., **41** (1937), 375–481.

UNIVERSITY OF MISSOURI