CONSTRUCTION OF THE LATTICE OF COMPLEMENTED IDEALS WITHIN THE UNIT GROUP

J. ELDON WHITESITT

In his book "Linear algebra and projective geometry" [1, pp. 203–227], R. Baer shows that in the ring of endomorphisms of a linear manifold, (F, A), except where the characteristic of F is 2, the projective geometry of the subspaces of the linear manifold is determined entirely within the multiplicative group of units in the ring. G. Ehrlich [2], using similar methods showed that the structure of a continuous geometry is determined within the unit group of the associated regular ring. The purpose of this paper is to show that a unified treatment may be given.

We will assume throughout that the ring R has an identity element which we denote by 1. We will say that a right ideal A in R is a *complemented right ideal* if there exists a right ideal A' such that $R = A \oplus A'$ where $\oplus$ indicates direct sum. We refer to such an ideal by the abbreviation C. R. I.

If K is any ring with identity, we denote the *unit group* of K by $U(K)$. Where K is R, this will be shortened to just U. For any set S of elements in R, we let $Z(S)$ denote the *center* of S, that is, the set of all those elements of S which commute with every element in S.

We assume the ring R satisfies the following postulates:

1. The mapping $r \to r + r$ for every element $r \in R$ is an automorphism of the additive group of R onto R. [1, p. 203; 2, p. 9]

This postulate requires a little more than that the characteristic of R is different from 2. We will denote $r+r$ by $2r$ and the inverse image of r by $\frac{1}{2}r$.

2. If A and B are C. R. I.'s then $A \cap B$ and $A \cup B$ are C. R. I.'s. [1, pp. 178, 179; 2, p. 6]

3. If e is a nonzero idempotent in R and if k is any element of R, then either $eRk=0$ or $kRe=0$ implies that $k=0$. [1, p. 198; 2, p. 16]

4. If e is an idempotent element of R, then $Z(U(eRe)) \leqq Z(eRe)$. [1, p. 201; 2, p. 14]

5. $Z(R)$ contains no nonzero divisors of zero. [1, p. 202; 2, p. 7]

An element of $u \in R$ is termed an *involution* if $u^2=1$. An element $s \in R$ which is the product of two distinct involutions and satisfies the property that $(s-1)^2=0$ is said to be of class two. Section 1 deals with

Received October 24, 1955. This paper contains the principal contents of a doctoral dissertation presented at the University of Illinois in June, 1954.

elements of class two, showing that they may be characterized within the unit group.

If a is any element of R, we define $J^+(a)$ to be the set of all $x \in R$ satisfying $ax=x$, and $J^-(a)$ to be the set of all $y \in R$ satisfying $ay=-y$. Then if A is a C. R. I. we define $\Delta(A)^+$ to be the set of all involutions u such that $A=J^+(u)$ and $\Delta(A)^-$ to be the set of all involutions v such that $A=J^-(v)$. Either of these sets is called a *Δ-set*. In § 2, *Δ-sets* are characterized within the unit group, making use of the results of § 1. It is shown that a one-to-one correspondence exists between the set of all C. R. I.'s and the set of all pairs $[\Delta(A)^+, \Delta(A)^-]$ of all Δ-sets, called *Δ-systems*.

Finally, it is shown in § 3 that the set of C. R. I.'s forms an irreducible, complemented modular lattice and that the ordering in the lattice is determined by the ordering of the Δ-systems, and conversely.

1. Elements of class two. It will be necessary to show that elements of class two can be characterized completely within the multiplicative group of units in the ring. First we list without proof some well-known properties of idempotent elements and the ideals they generate (complemented ideals) in the ring R. These results hold for arbitrary rings with 1. The proof of 1.1 is given in [**4**, p. 708].

PROPOSITION 1.1. (a) *An element e in R is idempotent if and only if $(1-e)$ is idempotent.*

(b) *If e is idempotent, eR is the set of elements x in R for which $ex=x$. Note that this implies that y is in $(1-e)R$ if and only if $ey=0$.*

(c) *If e and f are idempotents such that $eR=fR$, and $(1-e)R=(1-f)R$, then $e=f$.*

(d) *$R=A \oplus B$ for right ideals A and B if and only if there exists an idempotent e such that $eR=A$ and $(1-e)R=B$.*

The following result, useful for testing the equality of complemented right ideals, holds for arbitrary rings with 1. It is given in [**3**, p. 13].

PROPOSITION 1.2. *If e and f are idempotents, then $eR=fR$ if and only if $f=e+ex(1-e)$ for some $x \in R$.*

The following result, given in Ehrlich [**2**, pp. 9, 10] relates the set of all involutions to the set of all idempotents.

PROPOSITION 1.3. (a) *The mappings $u \to \frac{1}{2}(u+1)=e$ and $e \to 2e-1=u$ are one-to-one inverse mappings between the set of all involutions u and the set of all idempotents e in R.*

(b) *Similarly the mappings* $v \to \frac{1}{2}(1-v)=f$ *and* $f \to -2f+1=v$ *are one-to-one inverse mappings between these sets.*

(c) *For the involution* $u=2e-1$, $J^+(u)=eR$ *and* $J^-(u)=(1-e)R$.

It will be necessary to know that there exist "enough" involutions, or equivalently, idempotents.

LEMMA 1.4. *If* $A=eR=J^+(u)$ *for an idempotent* e *and involution* $u=2e-1$, *and if* $0<A<R$, *then there exists an idempotent* $f\neq e$ *such that* $A=fR$, *or equivalently, there exists an involution* $v\neq u$ *such that* $A=J^+(v)$.

Proof. Since $0<eR<R$, neither e nor $1-e$ is zero. By Postulate 3 there is an $x\in R$ such that $ex(1-e)\neq 0$. Let $f=e+ex(1-e)\neq e$. Then f is an idempotent and $eR=fR=A$. Equivalently, $v=2f-1$ is an involution such that $u\neq v$ and $A=J^+(v)$.

LEMMA 1.5. *If* $J^+(u)=J^+(v)=J^+(w)$ *for involutions* u, v, w, *then* $uvw=u-v+w$, *and* $(uv-1)^2=0$.

Proof. Let $A=J^+(u)=J^+(v)=J^+(w)$. Then $u+1$, $v+1$, and $w+1$ are in A. Hence

$$\begin{aligned} u-v+w &= u-(v+1)+(w+1)=u-u(v+1)+u(w+1)\\ &= u[1-(v+1)+(w+1)]=u[-v+w+1]\\ &= u[-v+v(w+1)]=uv(-1+w+1)=uvw\,. \end{aligned}$$

Now $uvu=2u-v$ and hence $(uv)^2=2uv-1$, or $(uv)^2-2uv+1=0$, that is, $(uv-1)^2=0$. This completes the proof.

In 1.1 we have seen that principal right ideals generated by idempotents are complemented, and it is necessary to know that certain other ideals are also complemented. In particular,

LEMMA 1.6. *If* $fR=eR$ *for idempotents* e, f, *then* $(f-e)R$ *is a* C. R. I.

Proof. We note that $fe=e$, $ef=f$ and $f=e+ez(1-e)$ for some $z\in R$. We will show that $(f-e)R=eR\cap[(1-e)R\cup(1-f)R]$. Clearly $(f-e)R\leq eR$ since $f-e=ez(1-e)$, and $(f-e)R\leq[(1-e)R\cup(1-f)R]$, since for any $x\in R$, $(f-e)x=(1-e)x+(1-f)(-x)$. Now suppose $y\in eR \cap[(1-e)R\cup(1-f)R]$, then $y=ey=(1-e)r_1+(1-f)r_2$, and $(1-e)y=0 =(1-e)r_1+(1-e)(1-f)r_2=(1-e)r_1+(1-e)r_2$. But then $y=(1-e)r_1 +(1-f)r_2=(1-e)r_1+(1-e)r_2+(f-e)(-r_2)=(f-e)(-r_2)$ and is in

$(f-e)R$. This shows $eR \cap [(1-e)R \cup (1-f)R] \leqq (f-e)R$, and hence equality holds. By Postulate 2, $(f-e)R$ is a C. R. I. This completes the proof.

PROPOSITION 1.7. *If u and v are involutions, then $J^+(uv)=J^+(vu) =[J^+(u) \cap J^+(v)] \oplus [J^-(u) \cap J^-(v)]$.*

Proof. Assume x is any element in $J^+(uv)$. This is equivalent to $uvx=x$, or $vx=ux$, or $x=vux$. Hence $J^+(uv)=J^+(vu)$. Further x may be written $x=x_u^+ + x_u^-$ where $x_u^+ \in J^+(u)$ and $x_u^- \in J^-(u)$. Then $ux=x_u^+ - x_u^-$ and $x+ux=2x_u^+$. Similarly, $x=x_v^+ + x_v^-$, where $x_v^+ \in J^+(v)$ and $x_v^- \in J^-(v)$, and $x+vx=2x_v^+$. Hence $x_u^+=x_v^+$ and $x_u^-=x_v^-$. That is, x is in $[J^+(u) \cap J^+(v)] \cup [J^-(u) \cap J^-(v)]$.

That $[J^+(u) \cap J^+(v)] \cup [J^-(u) \cap J^-(v)] \leqq J^+(uv)$ is clear and the sum is direct since $J^+(u) \cap J^-(u)=0$. This completes the proof.

We note that by Postulate 2, the above proposition also gives that $J^+(uv)$ is a C. R. I. Next we show that an element of class two may be written in a special form.

LEMMA 1.8. *If the element $s=u'v'$ for involutions u' and v' satisfies $(s-1)^2=0$, then there exist involutions u and v such that $s=uv$, and $J^+(u)=J^+(v)$.*

Proof. $(s-1)^2=0$ implies that $s(s-1)-(s-1)=0$ and hence that $s-1 \in J^+(s)$. Hence $(s-1)R \leqq J^+(s)$, and $J^+(s)$ is a C. R. I. by the preceding proposition. Now let u be any involution such that $(s-1)R \leqq J^+(u) \leqq J^+(s)$. This is possible, since $J^+(s)$ is a C.R.I. and will serve for $J^+(u)$. If $v=us$, $v=u(s-1)+u=s-1+u$, since $s-1 \in J^+(u)$.

$$v^2=(s-1)^2+(s-1)u+u(s-1)+u^2=(s-1)u+s-1+1=s(u+1)-(u+1)+1=1,$$

since $u+1 \in J^+(s) \leqq J^+(u)$. That is, v is an involution. Clearly $J^+(u) \leqq J^+(v)$. Assume that $x \in J^+(v)$, so that $x=vx=(s-1+u)x$. That is, $(s-1)x=(1-u)x$. But $(1-u)x \in J^-(u)$, while $(s-1)x \in J^+(u)$, and hence $(1-u)x=0$ for every $x \in J^+(v)$. That is, $J^+(v) \leqq J^+(u)$, and we have proved that equality holds. This completes the proof.

The following lemma, and the classification of elements of class two given in Theorem 1 are due to Israel Halperin. We define $C(s)$, the *centralizer* of an element $s \in R$, to be the set of all elements $t \in U$ such that $ts=st$. Then we let $C^2(s)=C(C(s))$ be the set of all elements in U which commute with every element in $C(s)$.

LEMMA 1.9. *If $s=1+n=uv$, where $n^2=0$ and u and v are involutions, then $nR=eR$ for some idempotent e, and for any such e, if $t \in C^2(s)$ and $te=et$, then $tx=xt$ for every $x \in U$.*

Proof. By 1.8 we may assume $J^+(u)=J^+(v)=iR$ for some idempotent i. Then $u=2[i+ix(1-i)]-1$ and $v=2[i+iy(1-i)]-1$ for some $x, y \in R$. Then by direct computation, $uv=1+iz(1-i)$, where $z=2(y-x)$. Hence $n=s-1=iz(1-i)=j-i$ for the idempotents $j=i+iz(1-i)$ and i, and nR is a C. R. I. by 1.6. Let $nR=eR$ for the idempotent e. Then $nR=eR \leqq iR$ implies $ie=e$, $(1-i)(1-e)=(1-i)$, $en=n$, $en(1-e)=n(1-e) =iz(1-i)(1-e)=n$, and $ne=0$.

Now $e=nh'$ for some $h' \in R$. Set $h=(1-e)h'e$, $g=hn$, $f=1-e-g$. Then $nh=n(1-e)h'e=nh'e=e$, $gn=0$, $ng=en=n$, $h=(1-e)he$, $h^2=0$, $hg=0$, $g^2=g$, $ge=eg=0$, $f^2=f$, $ne=nf=fn=gn=0$, and e, f, g are orthogonal idempotents satisfying $1=e+f+g$.

Further, $nx=0$ is equivalent to $gx=0$. Clearly $nx=0$ implies $gx=hnx =0$. $gx=0$ imples $x=(e+f)x$, hence $nx=n(e+f)x=n(1-g)x=0$.

Also $xn=0$ is equivalent to $xe=0$, since $eR=nR$.

Now let x be an arbitrary element in U. We show $xt=tx$ for any t in $C^2(s)$ for which $te=et$ by showing t commutes with each term in the expansion of $x=(e+f+g)x(e+f+g)$.

Since $fn=nf=0$ and $2f-1 \in U$, $2f-1$ is in $C(n)=C(s)$ and hence $tf=ft$. Then also $tg=gt$. $s^{-1}=n-1$, so $s \in U$, and hence $s \in C(s)$, and $ts=st$, $tn=nt$.

Using the relations given above between e, f, g, n, we have:

$1+exf$ has inverse $1-exf$ and is in $C(s)$, hence $texf=exft$.

$1+exg$ has inverse $1-exg$ and is in $C(s)$, hence $texg=exgt$.

$1+fxg$ has inverse $1-fxg$ and is in $C(s)$, hence $tfxg=fxgt$.

$1+exen$ has inverse $1-exen$ and is in $C(s)$, hence $texen=exent$, that is, $(texe-exet)n=0$, since $tn=nt$. But this is equivalent to $(texe-exet)e=0$ and hence $texe=exet$.

$1+fxen$ has inverse $1-fxen$ and is in $C(s)$, hence $tfxen=fxent$ and $tfxe=fxet$.

$1+nxn$ has inverse $1-fxen$ and is in $C(s)$, hence $tnxn=nxnt$, that is, $n(tx-xt)n=0$. But $ny=0$ is equivalent to $gy=0$, $zn=0$ is equivalent to $ze=0$, hence $tgxe=gxet$.

$1+nxf$ has inverse $1-nxf$ and is in $C(s)$, hence $tnxf=nxft$ and $tgxf=gxft$.

$1+nxg$ has inverse $1-nxg$ and is in $C(s)$, hence $tnxg=nxgt$ and $tgxg=gxgt$.

Finally, if $fyf \in U(fRf)$ with inverse $fzf \in fRf$, then $e+fyf+g$ has inverse $e+fzf+g$ in R and is in $C(s)$, hence $tfyf=fyft$ and $(ftf)(fyf)=(fyf)(ftf)$ and $ftf=tf$ has $t^{-1}f$ as inverse in fRf. Hence $ftf \in Z(U(fRf)) \leqq Z(fRf)$ by Postulate 4, and $tfxf=fxft$ for $x \in U$. This completes the proof.

The following theorem gives necessary and sufficient conditions that an element which is the product of two involutions be of class two. It will be noted that these conditions are entirely multiplicative in nature.

THEOREM 1. *If $s=uv$ for distinct involutions u, v, neither of which is ± 1, then s is of class 2 if and only if*

1. *For some $r \in U$, and involution w, we have*

$$wsw=s^{-1},$$

$$rsr^{-1}=s^2,$$

$$C(w) \leqq C(r), \text{ and}$$

$$C^2(s) \cap C(w) \leqq Z(U)$$

2. *$s^3 \neq 1$ or for every $s'=u'v'$ satisfying 1, $s'^3=1$.*

Proof. Assume $s=uv=n+1$, $n^2=0$, $n \neq 0$. Then as in 1.9, $nR=eR$ for an idempotent e, and $n=en$, $ne=0$. Let $r=1+e$, $w=2e-1$. Then $r^{-1}=1-e/2$, $w^2=1$, and $wsw=(2e-1)(1+n)(2e-1)=1-n=s^{-1}$. Further, we have that $rsr^{-1}=(1+e)(1+n)(1-e/2)=1+2n=1+2n+n^2=s^2$. If $yw=wy$, then $ye=ey$, and $yr=ry$, that is, $C(w) \leqq C(r)$. Finally, if $t \in C^2(s) \cap C(w)$, then $te=et$, and by 1.9, $t \in Z(U)$. (Note that t^{-1} exists since, for example, $C(w) \leqq U$). Hence we have established 1. We note that $s^3=1+3n$, but $3 \in Z(R)$, $n \neq 0$, and hence $s^3=1$ implies $3=0$.

Now assume $s=uv$ satisfies 1, 2. Let $t=s+s^{-1}$. Then $w(s+s^{-1})=s^{-1}+s$, that is, $wt=tw$. $C(w) \leqq C(r)$ implies that $tr=rt$ and $wr=rw$ since $w \in U$ and hence $w \in C(w)$. Hence $t=rtr^{-1}=rsr^{-1}+rs^{-1}r^{-1}=s^2+rwswr^{-1}=s^2+ws^2w=s^2+wswwsw=s^2+(s^{-1})^2=s^2+2+s^{-2}-2=(s+s^{-1})^2-2=t^2-2$. That is, $t^2-t-2=0$. Hence $t^{-1}=\frac{1}{2}(t-1)$ and t is in U, and in $C(w)$.

Now if $y \in C(s)$, $yt=ty$, and $t \in C^2(t)$. But then $t \in Z(U)$ and by Postulate 4, $t \in Z(R)$. Then $(t+1)$ and $(t-2)$ are in $Z(R)$. Hence $t^2-t-2=0=(t+1)(t-2)$ implies by Postulate 5 that $t=-1$ or $t=2$.

Suppose $t=s+s^{-1}=-1$. Then $s^2+s+1=0$. Multiplication by $s-1$ gives $s^3-1=0$, $s^3=1$, which contradicts 2 unless each $s'=u'v'$ satisfying 1 has the property $s'^3=1$. In this case, we show the existence of an element of class 2. Since $u \neq \pm 1$, $0 < J^+(u) < R$, and there exists an involution $u' \neq u$ such that $J^+(u)=J^+(u')$ by 1.4. Now by 1.5, $uu'=1+m$ is of class 2, hence satisfies 1, by the first part of this proof. Hence $3=0$ and $-1=2$.

Then in any case $t=2=s+s^{-1}$, hence $s^2-2s+1=(s-1)^2=0$. That is, s is of class 2 as was to be shown.

Finally, suppose $s=uv=1+n$, where $n^2=0$, $n \neq 0$, $s^3=1$. Then $3=0$

and if $s'=u'v'$ satisfies 1, by the preceding proof $t'-2=s'+s'^{-1}-2=0$, $s'^2-2s'+1=0$, and $(s'-1)^2=0$. Hence $s'^3=1+3n=1$, which completes the proof.

The cases where $u=v$, or one or both of u, v are 1 or -1 may be treated separately and the preceding theorem is easily seen to be true for each case. In these cases, s cannot be of class 2, and one or more of (1), (2) fails to hold in each case. These cases are not of interest, so the proofs are omitted.

2. Cosets of involutions. Having finished the characterization of elements of class two, we proceed with the discussion of the sets of involutions defined in the introduction, which we call Δ-sets. There are several simple properties which are apparent from the definition. We note that $\Delta(A)^-=-\Delta(A)^+$. If we define the *normalizer* of $\Delta(A)^+$, $N\Delta(A)^+$ to be the set of all involutions v such that $v\Delta(A)^+v\leqq\Delta(A)^+$, then $N\Delta(A)^+=N\Delta(A)^-$. We denote either of the latter by $N\Delta(A)$. If $A\neq 0$, then $\Delta(A)^+$ and $\Delta(A)^-$ have no elements in common. Further, if A and B are two C. R. I. such that $\Delta(A)^+$ and $\Delta(B)^+$ contain a common element, then $A=B$. It is clear that every involution u is in exactly one Δ-set, $\Delta[J^+(u)]^+=\Delta[J^-(u)]^-$. Finally we note that any Δ-set is completely determined by any one of its elements.

Let ϕ denote an arbitrary set of involutions. If ϕ satisfies certain properties (in particular if ϕ is a Δ-set) it will be shown that ϕ is a coset of involutions modulo the abelian subgroup ϕ^2 in u. This property is the justification for the term "coset of involutions" which heads this section.

PROPOSITION 2.1. *If the nonempty set ϕ of involutions satisfies the property that for every triple of involutions u, v, w in ϕ, $wvu=uvw$ is in ϕ, then ϕ^2 is an abelian subgroup of U and ϕ is a coset of involutions modulo ϕ^2, and conversely. Moreover, $wgw=g^{-1}$ for every w in ϕ, and every g in ϕ^2.*

If in addition, every element $s\neq 1$ of ϕ^2 is of class two, then every pair g, h, of elements in ϕ^2 satisfies the condition $(g-1)(h-1)=0$.

Proof. The first part of the proposition is quickly verified using the fact that if $g=uv\in\phi^2$, then $g^{-1}=vu$.

Now assume that g and h are any two elements of ϕ^2. Then $(g-1)^2=0$, or $g^2=2g-1$. Similarly, $h^2=2h-1$. But $gh=hg\in\phi^2$ and hence $0=(gh-1)^2=(2g-1)(2h-1)-2gh+1=4gh-2h-2g+1-2gh+1=2(g-1)(h-1)$, and hence $(g-1)(h-1)=0$, completing the proof.

The following Lemma, and its use in Theorem 2 are due to Israel Halperin.

LEMMA 2.2. *Let e be a fixed idempotent and let θ range over all involutions which commute with e. Suppose x arbitrary, but fixed. Then the principal right ideals $(\theta x)R$ have a least* C. R. I. *containing them and this* C. R. I. *is* 0, eR, $(1-e)R$, *or* R.

Proof. Let $u=2e-1$. For each θ, θu is an involution commuting with e. Hence the set $(\theta x)R$ include all the $(\theta ux)R$. Since $(\theta x)R \cup (\theta(2e-1)x)R = (\theta ex+\theta(1-e)x)R \cup (\theta ex-\theta(1-e)x)R=(\theta ex)R \cup (\theta(1-e)x)R$, we need only prove that the $(\theta ex)R$ have a least containing C. R. I. which is 0 or eR, and that the $(\theta(1-e)x)R$ have a least containing C. R. I. which is 0 or $(1-e)$R. By symmetry, we need only prove the first.

Now $(\theta ex)R \leqq eR$ for all θ. If eR is not the least containing C.R.I., (all $\theta exR) \leqq fR < eR$ for some idempotent f. Use efe in place of f so we can assume $fe=ef=f \neq e$. Then for every $y \in$ R, $g=f+(e-f)yf$ is an idempotent which commutes with e and satisfies $eg=g$, $fg=f$. Then $2g-1$ is a possible θ and so $(2g-1)ex=e(2g-1)x \in fR$ so that $e(2g-1)x=fe(2g-1)x$. That is, $(2g-e)x=fx$. But 1 is also a possible θ, so $ex=fex=fx$. Hence $2gx=2fx$ for all y. That is, $2(e-f)yfx=0$, and hence $(e-f)yfx=0$ for all $y \in R$. Since $e-f$ is a nonzero idempotent, by Postulate 3, $fx=0$. Hence $ex=fx=0$, and $(\theta ex)R=0$ for all θ. That is, we have shown that either eR or 0 is a least containing C. R. I.

The next step is to characterize Δ-sets within the unit group. It will be noted that in Theorem 2 all conditions are multiplicative in nature, using the results of Theorem 1.

THEOREM 2. *A nonvoid set of involutions ϕ is a Δ-set if and only if ϕ is a maximal family of involutions satisfying*

(a) *If u, v, w are in ϕ, then $uvw=wvu$ is in ϕ.*

(b) *If u, v are in ϕ, then there exists a unique $w \in \phi$ such that $wuw=v$.*

(c) *An involution u' is in $N\phi$ if and only if there exists an involution $u \in \phi$ such that $uu'=u'u$.*

(d) *Every $s \neq 1$ in ϕ^2 is of class 2.*

Further, if ϕ is a Δ-set containing more than one involution, ϕ uniquely determines a C. R. I., $A=J^+(\phi^2)$. *If ϕ contains exactly one involution, then this involution is* 1 *or* -1, *in both of which cases ϕ^2 coneists of* 1 *only and $J^+(\phi^2)=R$, though A may be* 0 *or* R.

Proof. Assume $\phi=\Delta(A)^+$, where A is a C. R. I. (The proof is similar if $\phi=\Delta(A)^-$.) By 1.5, if u, v, and w are in ϕ, $uvw=wvu$ and hence uvw is an involution. If $A=eR$ for an idempotent e, then by 1.2, 1.3, we have that $\frac{1}{2}(u+1)=e+ex(1-e)$, $\frac{1}{2}(v+1)=e+ey(1-e)$, $\frac{1}{2}(w+1)=e+ez(1-e)$ for some x, y, z in R. By direct computation, $uvw=2[e+e(x-y+z)(1-e)]-1$, and hence by 1.2 and 1.3 again, $J^+(uvw)=A$.

To establish (b), suppose that u and v are in $\phi=\Delta(A)^+$. Let $w=\frac{1}{2}(u+v)$, so that

$$w^2=\frac{1}{4}(u^2+uv+vu+v^2)=\frac{1}{4}(2+uvuu+vu)=\frac{1}{4}(2+(uvu+v)u)$$
$$=\frac{1}{4}(2+(2u-v+v)u)=\frac{1}{4}(2+2u^2)=1\ ,$$

using 1.5. So w is an involution, and clearly $A\leq J^+(w)$. Now if e, f, and g are the idempotents corresponding to u, v, and w as in 1.3 (a), then $J^+(w)=gR=\frac{1}{2}(w+1)R=\frac{1}{2}(e+f)R$, and since $eR=fR$, we have $J^+(w)\leq eR=J^+(u)$. Hence equality holds and $w\in\phi$. Now using 1.5 again, it is readily verified that $wuw=v$. To show uniqueness, assume w' is any involution in ϕ such that $w'uw'=v$. Then $w'uw'=wuw$, and by 1.5, $2w'-u=2w-u$, or $w'=w$.

To show that (c) holds, assume $u'\in N\phi$, and let v be any involution in ϕ. Then $u'vu'\in\phi$ by definition of $N\phi$. By (b), there exists $u\in\phi$ such that $u'vu'=uvu=2u-v$. Hence $v=2u'uu'-u'vu'=2u'uu'-2u+v$. That is, $2u'uu'=2u$, or $u'u=uu'$. For the converse, assume $u'u=uu'$ for some u in ϕ, and involution u'. We need to show that for every $v\in\phi$, $u'vu'\in\phi$. We note the equivalence of the following conditions: $y\in J^+(u'vu')$; $u'vu'y=y$; $vu'y=u'y$; $u'y\in J^+(v)=J^+(u)$; $uu'y=u'y$; $u'uu'y=y$; $uy=y$; $y\in J^+(u)$. Hence $u'vu'\in\phi$, and $u'\in N\phi$.

(d) is simply the second part of 1.5, and hence (a), (b), (c), (d) hold for an arbitrary Δ-set.

Now assume ϕ is a nonvoid maximal family of involutions satisfying (a), (b), (c), (d). If ϕ consists of 1 only, then $\phi=\Delta(R)^+$. If ϕ consists of -1 only, then $\phi=\Delta(R)^-$. In either case ϕ^2 consists of 1 only and $J^+(\phi^2)=R$. Next we will show that $\phi\leq\Delta(A)^+$ or $\phi\leq\Delta(A)^-$, where A is a C. R. I. Then the maximality of ϕ and the definition of Δ-set will imply equality.

If ϕ consists of exactly one involution u, then $\phi\leq\Delta(J^+(u))^+$ so we may assume ϕ contains two distinct involutions. Consider any $x\in R$, such that $ux=vx$ for a fixed u in ϕ and all v in ϕ. Form the set of all θx with θ ranging over all involutions commuting with u, or equivalently with $e=\frac{1}{2}(u+1)$. Then the $(\theta x)R$ have a least containing C.R.I. by 2.2 which is 0, eR, $(1-e)R$, or R. But as shown in 2.2, the set of

$(\theta x)R$ include the set of all $(\theta ux)R$, and hence if y ranges over all x such that $ux=vx$ for all $v\in\phi$, then the set of all $(\theta y)R$ also have a least containing C. R. I. which is 0, eR, $(1-e)R$, or R.

Now we show that the set of elements in the $(\theta y)R$, that is, the set B consisting of all θx, where θ is any involution commuting with u, and x satisfies $ux=vx$ for all v in ϕ, is identical with the set C consisting of all x such that $ux=vx$ for all $v\in\phi$. Clearly $C\leqq B$, since we may take $\theta=1$. But for any θ such that $u\theta=\theta u$ and x such that $ux=vx$ for all $v\in\phi$, we have $v(\theta x)=\theta\theta v\theta x=\theta w'x$, for some w' in ϕ, and continuing, $v(\theta x)=\theta ux=u(\theta x)$ so that θx is a possible x. That is $u(\theta x)=v(\theta x)$ for all $v\in\phi$. Thus $B=C$.

Now if we show that A, the least containing C. R. I. containing C is neither 0 nor R, then $A=eR$ or $A=(1-e)R$. That is, $A=J^+(u)$ or $A=J^-(u)$. But C is clearly independent of u, hence $A=J^+(v)$ or $A=J^-(v)$ for each $v\in\phi$.

Let u and v be any two distinct involutions in ϕ, w an arbitrary involution in ϕ. Then $uv\neq 1$ and $(wu-1)(uv-1)=0$ by 2.1. Hence $(u-w)(uv-1)=0$. That is, $x=uv-1\neq 0$ is an element such that $ux=wx$ for all $w\in\phi$. Hence $B\neq 0$, and $A\neq 0$.

Now if x satisfies $ux=vx$, $u\neq v$, then $x\in J^+(uv)$. That is, $C\leqq J^+(uv)$. But $J^+(uv)\neq R$ or $uv(1)=1$, and $u=v$, a contradiction. Hence we have proved that for every $v\in\phi$, $A=J^+(v)$ or $A=J^-(v)$.

Assume $A=J^+(u)=J^-(v)$ for some u, $v\in\phi$. Choose $x\neq 0$ in A. Then $ux=x$, $vx=-x$, $\frac{1}{2}(u+v)x=0$, and $\left(\frac{1}{2}(u+v)\right)^2x=0$. But by 2.1, $(uv-1)(vu-1)=0$, that is, $uv+vu=2$. Hence $\frac{1}{2}(u+v)$ is an involution and $\left(\frac{1}{2}(u+v)\right)^2x=x\neq 0$, a contradiction. Hence $A=J^+(w)$ for all $w\in\phi$, or $A=J^-(w)$ for all $w\in\phi$. That is, $\phi\leqq\Delta(A)^+$ or $\phi\leqq\Delta(A)^-$ and the assumption of maximality implies equality.

Now $J^+(\phi^2)=\bigcap J^+(uv)$ for all pairs uv in ϕ^2, or equivalently, $J^+(\phi^2)$ is the set of all x such that $uvx=x$ for every u, v in ϕ, or equivalently, the set of all x such that $ux=vx$ for all u, $v\in\phi$. Hence $J^+(\phi^2)$ $=C\leqq A$. Since $A=J^+(u)$ for all $u\in\phi$ or $A=J^-(u)$ for $u\in\phi$, $A\leqq J^+(\phi^2)$. Hence if ϕ contains more than one involution, a C. R. I., A, is uniquely determined by ϕ by the relation $J^+(\phi^2)=A$, and $\phi=\Delta(A)^+$ or $\phi=\Delta(A)^-$ $=-\Delta(A)^+$.

To complete the proof, we need only show that a nonvoid Δ-set ϕ, has the desired property of maximality. Assume $\phi\leqq\phi'$, and that ϕ' is a maximal family of involutions satisfying (a), (b), (c), (d). Then by the second part of this proof, ϕ' is a Δ-set which contains an element in common with the Δ-set ϕ. By definition of Δ-set, $\phi=\phi'$ which completes the proof of Theorem 2.

We have actually shown a little more than required in the proof of Theorem 2. We restate part of these results in the following form.

THEOREM 3. Mapping A onto $\Delta(A)$, and mapping $[\phi, -\phi]$ onto $J^+(\phi^2)$ constitute reciprocal and therefore one-to-one correspondences between the set of all nonzero complemented right ideals of the ring R and the set of all Δ-systems in the unit group of R.

3. The lattice of complemented right ideals. We have shown in the preceding sections that the complemented right ideals can be mapped in a one-to-one fashion upon the set of Δ-systems within the unit group. It remains to show that the set of C. R. I.'s form an irreducible, complemented, modular lattice and that the order relation in the lattice can be determined by an order relation among the Δ-systems, and conversely.

First, we state, without proof, a result given by Baer [1, p. 203] which depends only on Postulate 1.

LEMMA 3.1. *The following properties of an involution u and an element $a \in U$ are equivalent.*

(1) $au=ua$

(2) $aJ^+(u) \leqq J^+(u)$, *and* $aJ^-(u) \leqq J^-(u)$.

If A and B are C. R. I.'s such that $A \leqq B$, then any C. R. I., C, satisfying $B=A \oplus C$ is called a *relative complement* of A in B. The existence of relative complements is guaranteed by the following proposition.

PROPOSITION 3.2. If $fR \leqq eR$ and e, f are idempotents, then there exist idempotents i and j such that $eR=iR \oplus jR$, $fR=iR$, $ij=ji=0$, $ie=ei=i$, $je=ej=j$, and $e=i+j$.

Proof. Since $f \in eR$, $ef=f$ and $efe=fe$. Let $i=fe$. Then i is an idempotent which also generates fR. That is, $iR=fR$.

Let $j=e-i$. Then j is an idempotent in eR and $iR \cup jR=eR$. The relations $ie=ei=i$, $je=ej=j$, and $ij=ji=0$ are clear. We need only show the sum $iR \cup jR$ is direct. Since $ij=fe(e-fe)=fe-fe=0$, for any $x \in iR \cap jR$ we have $x=ix=ijx=0$. Hence the sum is direct which completes the proof.

We say a complemented lattice is irreducible if the zero and unit of the lattice (0 and R) are the only elements with unique complements. A stronger result can be shown, namely that relative complementation is also not unique except in trivial cases, but this will not be necessary.

THEOREM 4. *The complemented right ideals of R form an irreducible, complemented, modular lattice.*

Proof. That the set is a complemented modular lattice follows immediately from the definitions, Postulate 2, Proposition 1.1, and the fact that the modular law holds in the set of all right ideals and hence holds in the lattice. The lattice join is of course the ideal sum, $\cup$, and lattice meet is set theoretic intersection, $\cap$.

That the lattice is irreducible follows immediately from 1.4. If $0 < eR < R$, there exists $f \neq e$ such that $eR = fR$. Hence $(1-e)R$ and $(1-f)R$ are distinct complements of eR, by 1.1 (c).

The following lemma assures us of the existence of a particular type of complement.

LEMMA 3.3. *If $R = A \oplus B \oplus C$, where A, B, C are* C. R. I.'s, *and B, C are nonzero, then there exists a complement, $\overline{B}$, of B such that $A \leqq \overline{B}$ but $C \not\leqq \overline{B}$.*

Proof. It is an immediate consequence of 1.1 that there exist mutually orthogonal idempotents i, j, k, such that $A = iR$, $B = jR$, $C = kR$. By Postulate 3, there exists an $x \in R$ such that $jxk \neq 0$. Let $y = x(1-i)$. Then $jyk = jxk \neq 0$. Also $jyi = jx(1-i) = 0$.

Let $j' = j + jy(1-j)$. Then $jR = j'R$, $j'i = ji + jy(1-j)i = jyi = 0$, and $j'k = jk + jy(1-j)k = jyk \neq 0$. Hence k is not in $(1-j')R$ but i is in $(1-j')R$. Hence for $\overline{B} = (1-j')R$ we have $A \leqq \overline{B}$ and $C \not\leqq \overline{B}$, which completes the proof.

LEMMA 3.4. *If A and B are* C. R. I.'s, *then the following are equivalent:*

(1) $A \leqq B$ *or* $B \leqq A$

(2) $\Delta(A) \leqq N\Delta(B)$

(3) $\Delta(B) \leqq N\Delta(A)$

In (2) and (3), $\Delta(A)$ is understood to mean the set of all involutions in either $\Delta(A)^+$ or in $\Delta(A)^-$.

Proof. First we assume $A \leqq B$. Let u be any involution in $\Delta(A)^+$ and $e = \frac{1}{2}(u+1)$ so that $A = eR$. If $B = fR$ for the idempotent f, choose $g = f + fe(1-f) = f + e(1-f)$ since $A \leqq B$. Then $B = gR$ and $ge = e$. But $eg = ef + e(1-f) = e$. That is, $eg = ge$ and $uv = vu$ where $v = 2g-1$ is an involution in $\Delta(B)^+$. By Theorem 2 (c), $u \in N\,\Delta(B)$ and hence $\Delta(A)^+ \leqq N\Delta(B)$.

Next, let v be any involution in $\Delta(B)^+$, and $f=\frac{1}{2}(v+1)$ so that $B=fR$. By 3.2 there exists an idempotent e such that $A=eR$ and $ef=fe=e$. Hence if $u=2e-1$, $uv=vu$ where $u \in \Delta(A)^+$. By Theorem 2 (c), $v \in N\Delta(A)$ and hence $\Delta(B)^+ \leqq N\Delta(A)$. The case for $B \leqq A$ is clear by symmetry, and if we note that $\Delta(A)^- = -\Delta(A)^+$, and $\Delta(B)^- = -\Delta(B)^+$, we have shown that (1) implies (2) and (3).

Next we assume $A \not\leqq B$ and $B \not\leqq A$, and will show (2) and (3) fail to hold. There exist nonzero C. R. I.'s A' and B' such that $A=(A \cap B) \oplus A'$ and $B=(A \cap B) \oplus B'$ by 3.2. Then $A \cup B = (A \cap B) \oplus A' \oplus B'$. To show that this sum is direct we note that if $x \in B' \cap [(A \cap B) \cup A']$ then $x \in B'$ and $x \in (A \cap B) \cup A' = A \cap (B \cup A')$ by the modular law. That is, $x \in B' \cap (A \cap B)=0$. Interchanging A' and B' in this argument completes the proof that the sum is direct.

But $A \cup B$ is a C. R. I. by Postulate 2 and hence there exists a C. R. I. V such that $R=(A \cap B) \oplus A' \oplus B' \oplus V$. Further, by 3.3 there exists a complement $\overline{A'}$ of A' such that $(A \cap B) \oplus V \leqq \overline{A'}$ but $B' \not\leqq \overline{A'}$. Now choose idempotents h, i, j such that $A \cap B = hR$, $A' \oplus B' \oplus V =(1-h)R$; $A'=iR$, $\overline{A'}=(1-i)R$; $B'=jR$, and $(A \cap B) \oplus A' \oplus V=(1-j)R$. Then we note the following consequences of this choice:

(a) $ij \neq 0$ since $J \notin (1-i)R$.

(b) $ji=ih=hi=hj=jh=0$ since $i \in (1-j)R$, etc.

Now $h+i$ is an idempotent which generates A, and $w=2(h+i)-1$ is an involution such that $A=J^+(w)$. We show that $wj \notin B$. Otherwise, since $h+j$ generates B, $(h+j)wj=wj$, or equivalently, $(h+j)[2(h+i)-1]j =[2(h+i)-1]j$. Using (b) this reduces to $-j=2ij-j$ and hence $ij=0$ which contradicts (a). Hence $wj \notin B$.

We have found an involution $w \in \Delta(A)^+$ such that $wB \not\leqq B$, or equivalently $wJ^+(u) \not\leqq J^+(u)$ for any $u \in \Delta(B)^+$. By 3.1, $wu \neq uw$ for any $u \in \Delta(B)^+$, and hence by Theorem 2 (c), $\Delta(A) \not\leqq N\Delta(B)$. Exchanging A and B in the above argument shows $\Delta(B) \not\leqq N\Delta(A)$. This completes the proof of the equivalence of (1), (2), and (3).

LEMMA 3.5. *If e, f, g are mutually orthogonal idempotents where e, g are nonzero and such that $R=eR \oplus fR \oplus gR$, then an element $s \in U$ has the property $(s-1)R \leqq eR \leqq (e+f)R \leqq J^+(s)$ if and only if $s-1=exg$ for some x in R.*

Proof. Assume an element $s \in U$ has the property that $(s-1)R \leqq eR$ and $(e+f)R \leqq J^+(s)$. If we let $n=s-1$, the condition $(e+f)R \leqq J^+(s)$ is equivalent to $n(e+f)R=0$. Hence $n(e+f)=0$, and $n=n(1) =n(e+f+g)=ng$. Further, $nR \leqq eR$ implies $n=en$. Hence $n=en=eng$ as required.

Now assume $(s-1)=exg$ for some $x\in R$. Clearly $(s-1)R\leqq eR$. Let y be any element in $(e+f)R$. Then $(s-1)y=(s-1)(e+f)y=exg(e+f)y=0$. Hence $sy=y$, and $y\in J^+(s)$. This completes the proof.

COROLLARY 3.6. *If e, f, g are as in 3.5, then there exists an element $s\neq 1$ in U such that $s=uv$ for involutions u and v satisfying $J^+(u)=J^+(v)$ and such that $(s-1)R\leqq eR\leqq(e+f)R\leqq J^+(s)$.*

Proof. By Postulate 3, there exists an $x\in R$ such that $exg\neq 0$. Then $s=1+exg\neq 1$, and by 3.5 $(s-1)R\leqq eR\leqq(e+f)R\leqq J^+(s)$.

Next, $exg=2e\left(\frac{1}{2}\right)xg=2(1-g)e\left(\frac{1}{2}\right)xg$, since $eg=0$. Hence $exg=2[(1-g)+(1-g)\left(\frac{1}{2}ex\right)g-(1-g)]=2(h-k)$, where $k=1-g$ and h are idempotents generating the same ideal, $eR\oplus fR$. If $u=2h-1$, and $v=2k-1$, then u and v are involutions such that $J^+(u)=J^+(v)$ and hence $vu-1=v(u+1)-v-1=u+1-v-1=u-v$. Now $exg=2(h-k)=u-v=vu-1$. Then $s=1+exg=vu$ as required.

LEMMA 3.7. *Let A, B, and X be* C. R. I.'s. *Then*

(a) $0=A\cap B$, *or* $R=A\cup B$ *if and only if* $\Delta(A)^2\cap\Delta(B)^2=1$.

(b) $0<A\cap B\leqq X\leqq A\cup B<R$ *if and only if* $1<\Delta(A)^2\cap\Delta(B)^2\leqq\Delta(X)^2$.

Proof. First we prove the following: If $s\in U$, and A is a C. R. I. then $s=uv$ for involutions u and v such that $J^+(u)=J^+(v)$ is equivalent to $J^+(s)$ is a C. R. I. and $(s-1)R\leqq A\leqq J^+(s)$. To prove this, assume $s=uv$, where $J^+(u)=J^+(v)=A=eR$ for the idempotent e. $J^+(s)$ is a C. R. I. by 1.7. Also, as in the first paragraph of the proof of 1.9, $s-1=ez(1-e)$ for some $z\in R$. If the e, f, g of 3.5 are replaced by e, 0, $1-e$ respectively, then 3.5 gives $(s-1)R\leqq eR\leqq J^+(s)$. Conversely, assume $J^+(s)=gR$ for idempotent g and $(s-1)R\leqq A\leqq J^+(s)$. $s-1\in J^+(s)$ implies $(s-1)^2=0$. Now as in 1.8, and u and v exist such that $s=uv$ and $J^+(u)=J^+(v)=A$. This completes the proof of the statement, and as an immediate consequence we have,

(*) s is in $[\Delta(A)^2\cap\Delta(B)^2]$ if and only if $s=uv$ for involutions u, v, $(s-1)R\leqq A\cap B$, and $A\cup B\leqq J^+(s)$.

To establish (a) of the lemma, assume first $A\cap B=0$. By (*), $(s-1)R=0$ for every $s\in\Delta(A)^2\cap\Delta(B)^2$ and hence $s=1$. Next if $A\cup B=R$, then by (*), $J^+(s)=R$ for every $s\in\Delta(A)^2\cap\Delta(B)^2$, and hence $s=1$.

Suppose $\Delta(A)^2\cap\Delta(B)^2=1$, and assume by way of contradiction that $0<A\cap B$, and $A\cup B<R$. There exist mutually orthogonal idempotents e, f, and g such that $A\cap B=eR$, $(e+f)R=A\cup B$, and $R=eR$

$\oplus fR \oplus gR$. Since e and g are nonzero, by 3.6 there exists an $s=uv \neq 1$ for involutions u and v such that $(s-1)R \leqq A \cap B$ and $A \cup B \leqq J^+(s)$. By $(*)$, s is in $\Delta(A)^2 \cap \Delta(B)^2$, which is a contradiction. Hence either $A \cap B=0$, or $A \cup B=R$, which completes the proof of (a).

Now assume $0<A \cap B \leqq X \leqq A \cup B<R$. By (a), $1<\Delta(A)^2 \cap \Delta(B)^2$. Let s be any element of $\Delta(A)^2 \cap \Delta(B)^2$. Then by $(*)$, $(s-1)R \leqq A \cap B$, and $A \cup B \leqq J^+(s)$. Hence $(s-1)R \leqq X \leqq J^+(s)$. By the first statement of this proof, $s \in \Delta(X)^2$.

Conversely, assume $1<\Delta(A)^2 \cap \Delta(B)^2 \leqq \Delta(X)^2$. By (a), $0<A \cap B$ and $A \cup B<R$. Let e, f, g be chosen as in the proof of (a) and we will complete the proof in two steps by indirect arguments.

Suppose first that $A \cap B \not\leqq X$. Let $X'=X \cap A \cap B$ and denote by C the relative complement of X' in $A \cap B$. Then $C \cap X=0$, and $C \neq 0$. By 3.2, orthogonal idempotents i and j exist such that $C=iR$, $X'=jR$ and $i+j=e$. Then i, $(j+f)$, g are mutually orthogonal and i, g are nonzero. By 3.6 there exists an $s'=u'v' \neq 1$ for involutions u', v' such that $0 \neq (s'-1)R \leqq iR \leqq (1+j+f)R \leqq J^+(s')$. By $(*)$, $s' \in \Delta(A)^2 \cap \Delta(B)^2$. But $(s'-1)R \not\leqq X$ since $iR \cap X=0$. Hence $s' \notin \Delta(X)^2$, a contradiction, and hence $A \cap B \leqq X$.

Next assume $X \not\leqq A \cup B$. Since $gx=0$ is equivalent to $x \in (1-g)R =A \cup B$, there exists $x' \in X$ such that $gx' \neq 0$. By Postulate 3 there is an element $y \in R$ such that $eygx' \neq 0$. By 3.5, $s'=1+eyg$ satisfies the conditions $(s'-1)R \leqq A \cap B$ and $A \cup B \leqq J^+(s')$. By 3.6 and $(*)$, $s' \in [\Delta(A)^2 \cap \Delta(B)^2]$. But $X \not\leqq J^+(s')$ since $x' \in X$ and $sx'=x'+eygx' \neq x'$. By 1.8. $s' \notin \Delta(X)^2$, a contradiction. Hence $X \leqq A \cup B$, which completes the proof.

If A, B, and X are C. R. I.'s, we say X is between A and B if $A \leqq X \leqq B$, or $B \leqq X \leqq A$. Betweenness of C. R. I.'s is characterized within the unit group by the following theorem.

THEOREM 5. *If A, B and X are* C. R. I.'s *in R, then A and B are both different from 0 and R and X is between A and B if and only if*

(a) $\Delta(A) \leqq N\Delta(B)$, *or equivalently* $\Delta(B) \leqq N\Delta(A)$.

(b) $1<[\Delta(A)^2 \cap \Delta(B)^2] \leqq \Delta(X)^2$.

Proof. Suppose first that neither A nor B is 0 or R and X is between A and B. We may assume $0<A \leqq X \leqq B<R$. Then 3.4 and 3.7 give conditions (a) and (b).

Conversely, assume (a) and (b) hold. (a) implies by 3.4 that $A \leqq B$ or $B \leqq A$. Suppose $A \leqq B$. Then by (b) of 3.7 we have $0<A \leqq X \leqq B<R$. If $B \leqq A$ we have a similar result. This completes the proof.

Theorems 1, 2, 3, 5 show that the lattice of C. R. I.'s can be constructured within the unit group of the ring and that the order relation in the lattice is completely determined by the order relations among the structures $\Delta(A)$ and $N\Delta(A)$ in the unit group, and conversely.

REFERENCES

1. Reinhold Baer, *Linear algebra and projective geometry*, Academic Press, New York, 1952.

2. Gertrude Ehrlich, *The structure of continuous rings*, Dissertation, University of Tennessee, 1953.

3. John von Neumann, *Continuous geometry*, (Notes by L. R. Wilcox on lectures at the Institute for Advanced Study). Vol. 2, planographed, Edwards Brothers, Ann Arbor, 1937.

4. ———, *On regular rings*, Proc. Nat. Acad. Sci., **23** (1937), 707–713.

MONTANA STATE COLLEGE