On Regular Rings
Author(s): John Von Neumann
Source: *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 22, No. 12 (Dec. 15, 1936), pp. 707-713
Published by: National Academy of Sciences
Stable URL: https://www.jstor.org/stable/86608
Accessed: 12-02-2019 07:48 UTC

ON REGULAR RINGS

By John von Neumann

Princeton, N. J.

Communicated November 6, 1936

Introduction. 1. In what follows we shall consider rings $\mathfrak{R}$ (which are associative but not necessarily commutative) with unit 1—cf. v.d.W.[1] I., pp. 37–40. The theory of *semi-simplicity* of these $\mathfrak{R}$ has always been carried out on the basis "Chain-condition" or "Minimum-condition"—cf. v.d.W. II, p. 151, for semi-simplicity *Ibid.*, pp. 156–172. The object of this note is to give a theory of "regularity" of $\mathfrak{R}$, this notion being equivalent to semi-simplicity when the chain-condition is fulfilled, but possessing most essential features of the semi-simple theory quite independently of the chain-condition. In a subsequent note we will use these results to establish connections between abstract algebra and the "continuous geometries" introduced by the author in two earlier notes in these Proceedings.

It is defined by a simple algebraical condition, which seems to be new even as a criterion of semi-simplicity (when the chain-condition is required). Our method is purely algebraical, but a greater stress is laid on the lattice-theoretical[2] aspect of right- and left-ideals.

Definition of Regularity. 2. We define as usual (v.d.W. II, pp. 53–54):

Definition 1. A right (left) ideal—abbreviated: r.(l.)i.—is a set $\mathfrak{a} \subset \mathfrak{R}$ such that α) $x,y\epsilon\mathfrak{a}$ imply $x + y\epsilon\mathfrak{a}$, β) $x\epsilon\mathfrak{a}$, $z\epsilon\mathfrak{R}$ implies $xz\epsilon\mathfrak{a}$ ($zx\epsilon\mathfrak{a}$). If $a\epsilon\mathfrak{R}$ then a unique minimal r.(l.)i. exists, which contains a: The *principal right (left) ideal*—abbreviated: p.r.(l.)i.—of a, that is the set $(a)_r$ ($(a)_l$) of all az (za), $z\epsilon\mathfrak{R}$.

All statements we make for r. and for l.i. remain true if we interchange r. and l.

The following statements are evident: The r.i. form a partially ordered set with respect to set-theoretical inclusion $\mathfrak{a} \subset \mathfrak{b}$. This set has a minimum element: $(0) = (0)_r$ and a maximum one: $\mathfrak{R} = (1)_r$. For any set of r.i. $\mathfrak{a},\mathfrak{b},\ldots$ a maximum r.i. $\subset \mathfrak{a},\mathfrak{b},\ldots$ exists: The set-theoretical intersection of $\mathfrak{a},\mathfrak{b},\ldots$—*gr.l.b.*$(\mathfrak{a},\mathfrak{b},\ldots)$. Similarly a minimum r.i. $\supset \mathfrak{a},\mathfrak{b},\ldots$ exists: The set-theoretical intersection of all r.i. $\supset \mathfrak{a},\mathfrak{b},\ldots$—*l.u.b.*$(\mathfrak{a},\mathfrak{b},\ldots)$.

Definition 2. Write $\mathfrak{a} \cup \mathfrak{b} =$ *gr.l.b.* $(\mathfrak{a},\mathfrak{b})$, $\mathfrak{a} \cup \mathfrak{b} =$ *l.u.b.* $(\mathfrak{a},\mathfrak{b})$. Thus the r.i. form a *lattice* with *meet* $\mathfrak{a} \cap \mathfrak{b}$ and *join* $\mathfrak{a} \cup \mathfrak{b}$, *zero* (0), *unit* $\mathfrak{R}$ (cf. G. Birkhoff[2] p. 442) Two r.i. $\mathfrak{a},\mathfrak{b}$ are *inverses* if $\mathfrak{a} \cap \mathfrak{b} = (0)$, $\mathfrak{a} \cup \mathfrak{b} = \mathfrak{R}$. (Similarly for l.i.)

Clearly $\mathfrak{a} \cup \mathfrak{b}$ is the set of all $x + y$, $x\epsilon\mathfrak{a}$, $y\epsilon\mathfrak{b}$.

Definition 3. An element $e\epsilon\mathfrak{R}$ is *idempotent*—abbreviated: ip.—if $e^2 = e$.

We establish some basic properties of these notions.

Lemma 1. e is ip. if, and only if, $1 - e$ is ip.—*Proof:* $e^2 = e$ means $e(1 - e) = 0$ which is symmetric in e and $1 - e$.

Lemma 2. For an ip. e, $x\epsilon(e)_r$ means $ex = x$.—*Proof:* As $ex\epsilon(e)_r$, the condition is sufficient; as $x\epsilon(e)_r$ implies $x = ey$, $ex = e^2y = ey = x$, it is necessary.

Lemma 3. $\mathfrak{a},\mathfrak{b}$ are inverse r.i. if and only if $\mathfrak{a} = (e)_r$, $\mathfrak{b} = (1 - e)_r$ for a suitably chosen ip. e.—*Proof:* Sufficiency: As $1 = e + (1 - e)\ \epsilon\mathfrak{a} \cup \mathfrak{b}$ so $\mathfrak{a} \cup \mathfrak{b} = \mathfrak{R}$. $x\epsilon\mathfrak{a} \cap \mathfrak{b}$ implies $ex = x$ and $(1 - e)x = x$, $ex = 0$, so $x = 0$. Hence $\mathfrak{a} \cap \mathfrak{b} = (0)$.—Necessity: Let $\mathfrak{a},\mathfrak{b}$ be inverse r.i. Then $1 = x + y$, $x\epsilon\mathfrak{a}$, $y\epsilon\mathfrak{b}$. If $z\epsilon\mathfrak{a}$ then $z = xz + yz$, and $xz\epsilon\mathfrak{a}$ as $x\epsilon\mathfrak{a}$, so $yz\epsilon\mathfrak{a}$. But $yz\epsilon\mathfrak{b}$ as $y\epsilon\mathfrak{b}$ so $yz\epsilon\mathfrak{a} \cap \mathfrak{b}$, $yz = 0$. So $z = xz\epsilon(x)_r$. Thus $\mathfrak{a} \subset (x)_r$. Clearly $(x)_r \subset \mathfrak{a}$, so $\mathfrak{a} = (x)_r$. Similarly $\mathfrak{b} = (y)_r = (1 - x)_r$. Finally $x - x^2 = x(1 - x) = (1 - x)x\epsilon\mathfrak{a}$ and $\epsilon\mathfrak{b}$, so $\epsilon\ \mathfrak{a} \cap \mathfrak{b}$ so $= 0$. Thus x is ip., and is the desired e.

Lemma 4. The above $\mathfrak{a},\mathfrak{b}$ determine the ip. e uniquely.—*Proof:* That is: $(e)_r = (f)_r$, $(1 - e)_r = (1 - f)_r$, e,f ip., imply $e = f$. The first relation gives $e\epsilon(f)_r$, $fe = e$, $(1 - f)e = 0$. Replace e,f by $1 - e$, $1 - f$, so the second relation gives $f(1 - e) = 0$, $fe = f$. Hence $e = f$.

Lemma 5. $(a)_r = (e)_r$, e an ip., is equivalent to this: An x with $axa = a$ exists, and $e = ax$.—*Proof:* The condition is: $e\epsilon(a)_r$, e an ip., $a\epsilon(e)_r$. The first requirement means: $e = ax$; the second one: $e^2 = e$, that is $axax = ax$. Now the third one becomes: $ea = a$, that is $axa = a$. Since this implies the preceding equation, we have only $axa = a$, $e = ax$ left.

Lemma 6. The three following properties of a are equivalent to each other: α) An x with $axa = a$ exists. β) An ip. e with $(a)_r = (e)_r$ exists. γ) An r.i. $\mathfrak{b}$ which is inverse to $(a)_r$ exists.—*Proof:* β), γ) are equivalent by Lemma 3, α),β) are equivalent by Lemma 5.—

We now define:

Definition 4. $\mathfrak{R}$ is *regular* if for every $a\epsilon\mathfrak{R}$ an x with $axa = a$ exist. By Lemma 6, and owing to the symmetry of the above statement with respect to r. and l., it is equivalent to each one of the following conditions: α) An ip. e with $(a)_r = (e)_r$ exists. β) An ip. f with $(a)_l = (f)_l$ exists. γ) An r.i. $\mathfrak{b}$ which is inverse to $(a)_r$ exists. δ) An l.i. $\mathfrak{c}$ which is inverse to $(a)_l$ exists.

The form α) of our regularity-definition makes it clear that it coincides with semi-simplicity whenever the chain-condition holds. Indeed: Assume α). If $\mathfrak{a}$ is an r.i. $\neq (0)$ choose an $a \neq 0$ with $a\epsilon\mathfrak{a}$ and an ip. e with $(a)_r = (e)_r$. Then $a \neq 0$ gives $e \neq 0$ and $e\epsilon(e)_r = (a)_r = \mathfrak{a}$, $e = e^n\epsilon\mathfrak{a}^n$, so $\mathfrak{a}^n \neq (0)$, $\mathfrak{a}$ is not nilpotent. Conversely, assume the semi-simplicity of $\mathfrak{R}$ and the chain-condition. Then every "minimum" r.i. of $\mathfrak{R}$ fulfils α) by v.d.W. II, p. 157 ("Hilfssatz 3"), and this extends to all r.i. by the method *Ibid.*, p. 158 ("Satz 1," replace $\mathfrak{o} = \mathfrak{R}$ by the r.i. in question). We see, incidentally, that all r.i. in $\mathfrak{R}$ are principal, which is not generally true without the chain-condition.

It seems to be worth emphasizing that our definition of regularity by $axa = a$ is obviously r.-l.-symmetric, which the usual definition of semi-simplicity is not, and that it exhibits a remarkable similarity to the requirement of the existence of an "inverse element" ($ax = xa = 1$) in division-algebras.

Principal Right- and Left-Ideals. 3. From now on we assume $\mathfrak{R}$ to be regular, and denote the sets of all p.r.(l.)i. by $R_{\mathfrak{R}}$ ($L_{\mathfrak{R}}$). We will establish an important correspondence between $R_{\mathfrak{R}}$ and $L_{\mathfrak{R}}$. Again all statements arising from the ones which we will formulate by interchanging r. and l. will be true too.

Definition 5. If $\mathfrak{a}$ is an r.(l.)i., then let $\mathfrak{a}^l(\mathfrak{a}^r)$ be the set of all x for which $y\epsilon\mathfrak{a}$ implies $xy = 0$ ($yx = 0$).

Lemma 7. $\mathfrak{a}^l$ is an l.i.—*Proof:* Obvious.

Lemma 8. $\mathfrak{a} \subset \mathfrak{b}$ implies $\mathfrak{a}^l \supset \mathfrak{b}^l$.—*Proof:* Obvious.

Lemma 9. $\mathfrak{a} \subset \mathfrak{a}^{lr}$.—*Proof:* Obvious.

Lemma 10. $\mathfrak{a}^l = \mathfrak{a}^{lrl}$.—*Proof:* Apply ^{l} to Lemma 9; then $\mathfrak{a}^l \supset \mathfrak{a}^{lrl}$ results by Lemma 8. Interchange r. and l. in Lemma 9 and then apply it to $\mathfrak{a}^l$ then $\mathfrak{a}^l \subset \mathfrak{a}^{lrl}$ results. Hence $\mathfrak{a}^l = \mathfrak{a}^{lrl}$.

Lemma 11. For every p.r.i. $\mathfrak{a}$ a p.l.i. $\mathfrak{b}$ with $\mathfrak{a} = \mathfrak{b}^r$ exists.—*Proof:* By Definition 4, $\mathfrak{a} = (e)_r$ for an ip. e. So $x\epsilon\mathfrak{a}$ means $ex = x$, $(1 - e)\,x = 0$, that is $z(1 - e)x = 0$ for all $z\epsilon_{\mathfrak{R}}$. That is $yx = 0$ for all $y\epsilon(1 - e)_l$, so $\mathfrak{a} = (1 - e)_l^r$. So $\mathfrak{b} = (1 - e)_l$ has the desired properties.

Lemma 12. If $\mathfrak{a}$ is a p.r.i., then $\mathfrak{a} = \mathfrak{a}^{lr}$.—*Proof:* By Lemma 11. $\mathfrak{a} = \mathfrak{b}^r$ for a p.l.i. $\mathfrak{b}$. Interchange r. and l. in Lemma 10, then $\mathfrak{a}^{lr} = \mathfrak{b}^{rlr} = \mathfrak{b}^r = \mathfrak{a}$ results.

Lemma 13. If $\mathfrak{a}$ is a p.r.i., then $\mathfrak{a}^l$ is a p.l.i.—*Proof:* By Lemma 11. $\mathfrak{a} = \mathfrak{b}^r$ for a p.l.i. $\mathfrak{b}$. Interchange r. and l. in Lemma 12. Then $\mathfrak{a}^l = \mathfrak{b}^{rl} = \mathfrak{b}$ results.—

By Lemma 13 (and its r.-l.-transposed) $\mathfrak{a} \longrightarrow \mathfrak{a}^r$ maps $R_{\mathfrak{R}}$ on part of $L_{\mathfrak{R}}$ and $\mathfrak{a} \longrightarrow \mathfrak{a}^l$ maps $L_{\mathfrak{R}}$ on part of $R_{\mathfrak{R}}$. By Lemma 12 (and its r.l.-transposed) these mappings are inverse to each other, hence one-to-one correspondences of $R_{\mathfrak{R}}$ and $L_{\mathfrak{R}}$. By Lemma 8 they are anti-monotonic. So we have proved:

Theorem 1. $\mathfrak{a} \longrightarrow \mathfrak{a}^l$ is a one-to-one mapping of $R_{\mathfrak{R}}$ on $L_{\mathfrak{R}}$, $\mathfrak{a} \longrightarrow \mathfrak{a}^r$ is a one-to-one mapping of $L_{\mathfrak{R}}$ on $R_{\mathfrak{R}}$. They are inverse to each other, and anti-monotonic.

4. We show now that $R_{\mathfrak{R}}$ and $L_{\mathfrak{R}}$ are lattices.[3]

Lemma 14. If $\mathfrak{a},\mathfrak{b}$ are p.r.i., then two ip. e,f with $ef = fe = 0$ and $\mathfrak{a} \cup \mathfrak{b} = (e)_r \cup (f)_r$ exist.—*Proof:* By Definition 4, α), $\mathfrak{a} = (e_r)$, e ip. Besides $\mathfrak{b} = (b)_r$. Put $\mathfrak{b}_1 = ((1 - e)b)_r$. $\mathfrak{a} \cup \mathfrak{b}$ is the set of all $x + y$, $x\epsilon\mathfrak{a}$, $y\epsilon\mathfrak{b}$; that is, the set of all $eu + bv, u, v \epsilon \mathfrak{R}$. $\mathfrak{a} \cup \mathfrak{b}_1$, is the set of all $x + y$, $x \epsilon \mathfrak{a}$, $y \epsilon \mathfrak{b}_1$, that is the set of all $eu' + (1 - e)bv = e(u' - bv) + bv, u', v \epsilon \mathfrak{R}$. The correspondence $u = u' - bv, u' = u + bv$ shows that $\mathfrak{a} \cup \mathfrak{b} = \mathfrak{a} \cup \mathfrak{b}_1$.

By Definition 4, α), $\mathfrak{b}_1 = (f_1)_r$, f_1 ip. As $f_1 \epsilon \mathfrak{b}_1 = ((1 - e)b)_r$, so $f_1 = (1 - e)bw$, hence $ef_1 = 0$. Now put $f = f_1(1 - e)$. Then $ff_1 = f_1(1 - e)f_1 = f_1(f_1 - ef_1) = f_1 f_1 = f_1$. Hence $f^2 = ff_1(1 - e) = f_1(1 - e) = f, f$ ip. Since $f = f_1(1 - e) \epsilon (f_1)_r$, $f_1 = ff_1 \epsilon (f)_r$, so $(f)_r = (f_1)_r = \mathfrak{b}_1$. Hence $\mathfrak{a} \cup \mathfrak{b} = \mathfrak{a} \cup \mathfrak{b}_1 = (e)_r + (f)_r$.

Now $ef = ef_1(1 - e) = 0$, $fe = f_1(1 - e)e = 0$.

Lemma 15. If $\mathfrak{a}, \mathfrak{b}$ are p.r.i., then $\mathfrak{a} \cup \mathfrak{b}$ is a p.r.i. too.—*Proof:* Choose e, f as in Lemma 14. Then $e + f \epsilon (e)_r \cup (f)_r$, $(e + f)_r \subset (e)_r \cup (f)_r$. On the other hand $(e + f)e = e^2 + fe = e$, $(e + f)f = ef + f^2 = f$, hence e, $f \epsilon (e + f)_r$, $(e)_r$, $(f)_r \subset (e + f)_r$ and $(e)_r \cup (f)_r \subset (e + f)_r$. So $(e + f)_r = (e)_r \cup (f)_r = \mathfrak{a} \cup \mathfrak{b}$.

Lemma 16. If $\mathfrak{a}, \mathfrak{b}$ are p.r.i., then α) a minimum p.r.i. $\supset \mathfrak{a}, \mathfrak{b}$ exists, and it is $\mathfrak{a} \cup \mathfrak{b}$, β) a maximum p.r.i. $\subset \mathfrak{a}, \mathfrak{b}$ exists, and it is $\mathfrak{a} \cap \mathfrak{b}$.—*Proof:* Ad α): By Lemma 15. $\mathfrak{a} \cup \mathfrak{b}$ is a p.r.i., the other statements about $\mathfrak{a} \cup \mathfrak{b}$ are obvious. Ad β): Applying ^{r} to the p.l.i. $\mathfrak{a}^l, \mathfrak{b}^l$, and using Theorem 1, we see that the desired p.r.i. exists, and that it is equal to $(\mathfrak{a}^l \cup \mathfrak{b}^l)^r$. But this is equal to $\mathfrak{a}^{lr} \cap \mathfrak{b}^{lr}$ (obviously $(\mathfrak{c} \cup \mathfrak{d})^r = \mathfrak{c}^r \cap \mathfrak{d}^r$ for all l.i. $\mathfrak{c}, \mathfrak{d}$) that is to $\mathfrak{a} \cap \mathfrak{b}$ by Theorem 1 (or Lemma 12).—

Lemma 16, α), β), establish the lattice-character of $R_{\mathfrak{R}}$ with meet $\mathfrak{a} \cap \mathfrak{b}$ and join $\mathfrak{a} \cup \mathfrak{b}$. Clearly $(0) = (0)_r$ is the zero, and $\mathfrak{R} = (1)_r$ the unit. Definition 4, γ), secures for each p.r.i. $\mathfrak{a}$ an r.i. $\mathfrak{b}$ with $\mathfrak{a} \cap \mathfrak{b} = (0)$, $\mathfrak{a} \cup \mathfrak{b} = \mathfrak{R}$, and $\mathfrak{b}$ is a p.r.i. by Lemma 3. Hence $R_{\mathfrak{R}}$ is a "complemented" lattice (cf. G. Birkhoff,[4] p. 743, condition L 7, and footnote 3). Furthermore $R_{\mathfrak{R}}$ is a "modular" lattice (cf. G. Birkhoff[2], p. 445 where it is called a "B-lattice," and,[4] p. 743, condition L 5): (*) $\mathfrak{a} \subset \mathfrak{c}$ implies $(\mathfrak{a} \cup \mathfrak{b}) \cap \mathfrak{c} = \mathfrak{a} \cup (\mathfrak{b} \cap \mathfrak{c})$. Indeed: $(\mathfrak{a} \cup \mathfrak{b}) \cap \mathfrak{c} \supset \mathfrak{a} \cap \mathfrak{c} = \mathfrak{a}$ and $\supset \mathfrak{b} \cap \mathfrak{c}$; hence it is $\supset \mathfrak{a} \cup (\mathfrak{b} \cap \mathfrak{c})$. Next $x \epsilon (\mathfrak{a} \cup \mathfrak{b}) \cap \mathfrak{c}$ implies $x \epsilon \mathfrak{c}$ and $x \epsilon \mathfrak{a} \cup \mathfrak{b}$, that is $x = y + z$, $y \epsilon \mathfrak{a}$, $z \epsilon \mathfrak{b}$. Now $x \epsilon \mathfrak{c}$, $y \epsilon \mathfrak{a} \subset \mathfrak{c}$, so $z \epsilon \mathfrak{c}$, hence $z \epsilon \mathfrak{b} \cap \mathfrak{c}$, $x \epsilon \mathfrak{a} \cup (\mathfrak{b} \cap \mathfrak{c})$. Thus $(\mathfrak{a} \cup \mathfrak{b}) \cap \mathfrak{c} \subset \mathfrak{a} \cup (\mathfrak{b} \cap \mathfrak{c})$, proving (*).

Interchanging r. and l. establishes the same facts for $L_{\mathfrak{R}}$. Summing up, remembering Theorem 1:

Theorem 2. $R_{\mathfrak{R}}$ and $L_{\mathfrak{R}}$ are both *complemented, modular lattices,* with *meet* $\mathfrak{a} \cap \mathfrak{b}$, *join* $\mathfrak{a} \cup \mathfrak{b}$, *zero* (0), *unit* $\mathfrak{R}$. They are anti-isomorphic, the mappings of Theorem 1 being the anti-isomorphisms, interchanging $\subset$ and $\supset$, and consequently $\cup$ and $\cap$ too.

The Center. 5. Define as usual:

Definition 6. The center of $\mathfrak{R}$ is the set $\mathfrak{Z}$ of those $a \epsilon \mathfrak{R}$ which commute with every $x \epsilon \mathfrak{R}$: $ax = xa$.

$\mathfrak{Z}$ is a commutative ring with unit 1, and we prove:

Theorem 3. $\mathfrak{Z}$ is regular.—*Proof:* Consider an $a\epsilon\mathfrak{Z}$. As $\mathfrak{R}$ is regular, an $x\epsilon\mathfrak{R}$ with $axa = a$ exists. As a commutes with everything, so $a \cdot a^2x^3 \cdot a = axaxaxa = a$. Again $a^2x = xa^2 = axa = a$ commutes with everything, hence for every $z\epsilon\mathfrak{R}$, $x \cdot a^2z = xa^2 \cdot z = z \cdot xa^2 = a^2z \cdot x, a^2z$ commutes with x. Therefore x^3 commutes with it too, and so $a^2x^3 \cdot z = x^3 \cdot a^2z = a^2z \cdot x^3 = z \cdot a^2x^3$. Thus $x' = a^2x^3\epsilon\mathfrak{Z}$, and since $ax'a = a$, this establishes the regularity of $\mathfrak{Z}$.—

We discuss now those p.r.(l.)i. in $\mathfrak{R}$ which are generated by elements of $\mathfrak{Z}$. The same results hold for p.r.(l.)i. in $\mathfrak{Z}$ too: If we replace $\mathfrak{R}$ by $\mathfrak{Z}$ (which is permissible, since $\mathfrak{Z}$ is regular by Theorem 3), then the center remains $\mathfrak{Z}$.

Lemma 17. If $a\epsilon\mathfrak{Z}$ then $(a)_r = (a)_l$ and $(a)_r{}^l = (a)_l{}^r$. We denote this p.r. and p.l.i. by $(a)_*$ and $(a)_*{}^*$. *Proof:* As $ax = xa$ always, so $(a)_r = (a)_l$. $x\epsilon(a)_r{}^l$ means $xy = 0$ for all $y\epsilon(a)_r$, that is $xaz = 0$ for all z, that is $xa = 0$. $x\epsilon(a)_l{}^r$ means similarly $yx = 0$ for all $y\epsilon(a)_l$, that is $zax = 0$ for all z that is $ax = 0$. Now $xa = 0$ and $ax = 0$ are equivalent, hence $(a)_r{}^l = (a)_l{}^r$.

Lemma 18. α) A p.r.i. $\mathfrak{a}$ is at the same time an l.i. if and only if $\mathfrak{a} = (a)_*$ for an $a\epsilon\mathfrak{Z}$. We may even choose a as an ip. $e\epsilon\mathfrak{Z}$. β) If an l.i. $\mathfrak{a}$ is $= (e)_r$ for an ip. $e\epsilon\mathfrak{R}$, then this e is uniquely determined by $\mathfrak{a}$ and $e\epsilon\mathfrak{Z}$. Hence $\mathfrak{a} = (e)_*$.—*Proof:* Ad α): Sufficiency of $\mathfrak{a} = (a)_*, a\epsilon\mathfrak{Z}$: Obvious. Necessity of $\mathfrak{a} = (e)_*$, e an ip. $\epsilon\mathfrak{Z}$: As $\mathfrak{a}$ is a p.r.i., so $\mathfrak{a} = (e)_r$ for an ip. $e\epsilon\mathfrak{R}$ by Definition 4, α). Since $\mathfrak{a}$ is an l.i., so our β) gives $e\epsilon\mathfrak{Z}$, hence it suffices to prove β).

Ad β): Let $\mathfrak{a} = (e)_r$ be an l.i., e an ip. $\epsilon\mathfrak{R}$. Assume $x\epsilon\mathfrak{a}$. Then $x, e\epsilon\mathfrak{a}$, and as $\mathfrak{a}$ is an l.i., so $(x)_l$, $(e)_l$ and $(x)_l \cup (e)_l \subset \mathfrak{a}$. By Theorem 2 $(x)_l \cup (e)_l$ is a p.l.i., so it is $= (f)_l, f$ ip., by Definition 4, β). So $f\epsilon(f)_l \subset \mathfrak{a} = (e)_r$, hence $ef = f$, and $e\epsilon(e)_l \subset (x)_l \cup (e)_l = (f)_l$, hence $ef = e$. Thus $f = e$, $x\epsilon(x)_l \subset (x)_l \cup (e)_l = (f)_l = (e)_l$. Since this holds for all $x\epsilon\mathfrak{a}$ so $\mathfrak{a} \subset (e)_l$. But we have proved $(e)_l \subset \mathfrak{a}$ already; therefore $\mathfrak{a} = (e)_l$.

Now $\mathfrak{a} = (e)_r = (e)_l$ gives for every x: $exe\epsilon(e)_r = \mathfrak{a} = (e)_l$, hence $exe = ex$, and $xe\epsilon(e)_l = \mathfrak{a} = (e)_r$, hence $exe = xe$. Thus $ex = xe$ which proves that $e\epsilon\mathfrak{Z}$. So $\mathfrak{a} = (e)_*$.

If $\mathfrak{a} = (g)_r$ for another ip. g, then we have: $g\epsilon(g)_r = \mathfrak{a} = (e)_l$, hence $ge = g$, and $e\epsilon(e)_l = \mathfrak{a} = (g)_r$, hence $ge = e$. So $g = e$.

Lemma 19. The only *reductions* of $\mathfrak{R}$ that is its decompositions into two r. and l.i. direct summands (cf. v.d.W. II, pp. 161–162), are these: $\left(\substack{*\\ *}\right)$ $\mathfrak{R} = (e)_* + (1 - e)_*$, e an ip. $\epsilon\mathfrak{Z}$.—*Proof:* In other words: The only pairs of inverse sets $\mathfrak{a}, \mathfrak{b}$ (cf. Definition 2) which are both r. and l.i., are these: $\mathfrak{a} = (e)_*, \mathfrak{b} = (1 - e)_*$, e and ip. $\epsilon\mathfrak{Z}$. Sufficiency: Obvious. Necessity: $\mathfrak{a}, \mathfrak{b}$ are inverse r.i. so by Lemma 3, $\mathfrak{a} = (e)_r$, $\mathfrak{b} = (1 - e)_r$, e an ip. $\epsilon\mathfrak{R}$. As $\mathfrak{a}$ is l.i. too, so Lemma 18, β), gives $e\epsilon\mathfrak{Z}$. Hence $1 - e\epsilon\mathfrak{Z}$, $\mathfrak{a} = (e)_*$, $\mathfrak{b} = (1 - e)_*$.—

The *total reducibility* of $\mathfrak{R}$ would amount to this: For every r. and l.i. $\mathfrak{a}$ an inverse r. and l.i. $\mathfrak{b}$ can be found. (This is not the definition of v.d.W. II, pp. 161–162, which combines the above condition with the chain-condition). One can show by examples, however, that this is not always the case.

By Lemma 19 a necessary condition is that $\mathfrak{a}$ be even p.r.i. Conversely: If $\mathfrak{a}$ is p.r.i. (and also l.i.), then Lemma 18, α), gives $\mathfrak{a} = (e)_*$, e an ip. $\epsilon\mathfrak{Z}$, and so $\mathfrak{b} = (1 - e)_*$ is the desired inverse. So the p.r.i.- (or just as well the p.l.i.-) character of the r. and l.i. $\mathfrak{a}$ is necessary and sufficient for the existence of an inverse r. and l.i. $\mathfrak{b}$. Summing up:

Theorem 4. $\mathfrak{R}$ is *totally reducible* in the above restricted sense, and all *reductions* of $\mathfrak{R}$ are given by the ip. $e\epsilon\mathfrak{Z}$ in $(^*_*)$.—

We prove finally:

Theorem 5. $\mathfrak{R}$ is irreducible if and only if $\mathfrak{Z}$ is a division-algebra.—*Proof:* Owing to Lemma 19, the irreducibility of $\mathfrak{R}$ means that 0 and 1 are the only ip. $\epsilon\mathfrak{Z}$. Sufficiency of this condition: Let then a be $\epsilon\mathfrak{Z}$ and $\neq 0$. As $\mathfrak{Z}$ is regular, so $(a)_r = (e)_r$ in $\mathfrak{Z}$, e ip. $\epsilon\mathfrak{Z}$. $a \neq 0$ gives $e \neq 0$, so $e = 1$ $(a)_r = (1)_r = \mathfrak{Z}$ (in $\mathfrak{Z}$!), $1 = ax = xa$ for an $x\epsilon\mathfrak{Z}$. Thus a^{-1} exists in $\mathfrak{Z}$. Necessity: If $\mathfrak{Z}$ is a division-algebra, then for an ip. $e\epsilon\mathfrak{Z}$ we have $e(1 - e) = e - e^2 = 0$, so $e = 0$ or $1 - e = 0$, $e = 1$.

6. *Definition 7.* Let $Z_{\mathfrak{R}}$ be the intersection of $R_{\mathfrak{R}}$ and $L_{\mathfrak{R}}$.

By Lemma 18 $\mathfrak{a} = (e)_*$ establishes a one-to-one correspondence of all $\mathfrak{a}\epsilon Z_{\mathfrak{R}}$ and all ip. $e\epsilon\mathfrak{Z}$.

Lemma 20. If e is an ip. $\epsilon\mathfrak{R}$, then $(1 - e)xe = 0$ for all $x\epsilon\mathfrak{R}$ is equivalent to $e\epsilon\mathfrak{Z}$.—*Proof:* Sufficiency: If $e\epsilon\mathfrak{Z}$, then $(1 - e)xe = (1 - e)ex = 0$. Necessity: $(1 - e)xe = 0$, hence $exe = xe$, $xe\epsilon(e)_r$. As $(e)_r$ is an r.i., this implies $xey\epsilon(e)_r$, and as ey is the general element of $(e)_r$, so $u\epsilon(e)_r$ implies $xu\epsilon(e)_r$. That is: $(e)_r$ is an l.i. Hence $e\epsilon\mathfrak{Z}$ by Lemma 18, β).

Theorem 6. $Z_{\mathfrak{R}}$ is the set of those $\mathfrak{a}\epsilon R_{\mathfrak{R}}$ which possess a unique inverse $\mathfrak{b}\epsilon R_{\mathfrak{R}}$.—*Proof:* This means, owing to Lemmas 3 and 4: $\mathfrak{a}\epsilon Z_{\mathfrak{R}}$ if and only if $\mathfrak{a} = (e)_r$ for a unique ip. $e\epsilon\mathfrak{R}$. Sufficiency: $\mathfrak{a}\epsilon Z_{\mathfrak{R}}$ implies this by Lemma 18, β). Necessity: Assume $\mathfrak{a} = (e)_r$ for a unique ip. $e\epsilon\mathfrak{R}$. Put $e_1 = e + ex(1 - e)$. Then $e_1e = e$, hence $e\epsilon(e_1)_r$ and $ee_1 = e_1$, hence $e_1\epsilon(e)_r$. So $\mathfrak{a} = (e)_r = (e_1)_r$. Besides $e_1{}^2 = e_1e_1 = e_1.ee_1 = e_1e.e_1 = ee_1 = e_1$, so e_1 ip. Hence $e_1 = e$, $ex(1 - e) = 0$. Now Lemma 20 (with $1 - e$ for e) gives $1 - e\epsilon\mathfrak{Z}$, $e\epsilon\mathfrak{Z}$.—

We have now characterized $Z_{\mathfrak{R}}$ in terms of the lattice $R_{\mathfrak{R}}$ (or just as well $L_{\mathfrak{R}}$) only. It would be easy to show that $Z_{\mathfrak{R}}$ is the set of all "neutral" elements in $R_{\mathfrak{R}}(L_{\mathfrak{R}})$ in the sense of O. Ore,[2] pp. 419–421.

Computation rules in the lattice $Z_{\mathfrak{R}}$:

Lemma 21. The unique inverse of $(e)_*$, e an ip. $\epsilon\mathfrak{Z}$, is $(e)_*{}^* = (1 - e)_*$ (cf. Lemma 17).—*Proof:* $(1 - e)_*$ is inverse to $(e)_*$ by Lemma 3, unique by Theorem 6. $(e)_*^*$ is (cf. the proof of Lemma 17) the set of all x with $ex = 0$, that is $(1 - e)x = x$; hence it is equal to $(1 - e)_*$.

Lemma 22. If e,f are ip. $\epsilon\mathfrak{Z}$ then ef is too, and $(e)_* \cap (f)_* = (ef)_*$.—*Proof:* $ef\epsilon\mathfrak{Z}$ as $e,f\epsilon\mathfrak{Z}$, and $(ef)^2 = efef = eeff = ef$, so ef ip. $ef = fe$ is $\epsilon(e)_*$ and $(f)_*$, so $(ef)_* \subset (e)_*$, $(f)_*$ and $\subset (e)_* \cap (f)_*$. And $x\epsilon(e)_* \cap (f)_*$ gives $ex = fx = x$, so $efx = x$, $x\epsilon(ef)_*$. Hence $(e)_* \cap (f)_* \subset (ef)_*$. So $(e)_* \cap (f)_* = (ef)_*$.

Lemma 23. If e,f are ip. $\epsilon\mathfrak{Z}$ then $e + f - ef$ is too, and $(e)_* \cup (f)_* = (e + f - ef)_*$.—*Proof:* $e + f - ef = 1 - (1 - e)(1 - f)$ is an ip. $\epsilon\mathfrak{Z}$ along with e,f. By Theorem 2, $(e)_* \cup (f)_* = ((e)_*^* \cap (f)_*^*)^* =$ (* coincides here with ^{r,l}) $= (1 - (1 - e)(1 - f))_* = (e + f - ef)_*$.—

It is now easy to verify that $Z_{\mathfrak{R}}$ is a distributive lattice or a *Boolean algebra,* that is, that for all ip. $e,f,g\epsilon\mathfrak{Z}$ the distributive law $((e)_* \cup (f)_*) \cap (g)_* = ((e)_* \cap (g)_*) \cup ((f)_* \cup (g)_*)$ holds. Indeed: By Lemmas 22–23 both sides are equal to $(eg + fg - efg)_*$. Se we see:

Theorem 7. $Z_{\mathfrak{R}}$ is a *complemented Boolean algebra.*

Remarks. 7. *Definition 8.* Given an ip. e let $\mathfrak{R}(e)$ be the set of all $x\epsilon\mathfrak{R}$ with $ex = xe = x$. Given an $n = 1,2,\ldots$ let $\mathfrak{R}_n$ be the set of all nth order matrices (x_{ij}) $i,j = 1,\ldots, n$ of elements $x_{ij}\epsilon\mathfrak{R}$.[5] Clearly $\mathfrak{R}(e)$ is a ring with unit e, and $\mathfrak{R}_n$ is a ring with unit $1_n = (\delta_{ij})$ $\delta_{ij} = 1$ for $i = j$ and $= 0$ for $i \neq j$.

$\mathfrak{R}(e)$ is regular: If $a\epsilon\mathfrak{R}(e)$ then an $x\epsilon\mathfrak{R}$ with $axa = a$ exists. Now $e \cdot exe = exe = exe \cdot e$, hence $x' = exe\epsilon\mathfrak{R}(e)$, and $ax'a = a \cdot exe \cdot a = ae \cdot xea = axa = a$.

$\mathfrak{R}_n$ is regular too. We omit the proof, which is best based on a discussion of systems of linear equations in $\mathfrak{R}$ leading to a verification of Definition 4, γ, for $\mathfrak{R}_n$.

[1] B. L. van der Waerden, "Moderne Algebra," Vols. I and II. J. Springer, 1930, to be quoted as v.d.W. I and II, respectively.

[2] F. Klein, *Math. Ann.*, **105**, 308–323 (1931); G. Birkhoff, *Proc. Cambridge Phil. Soc.*, **29**, 441–464 (1933); O. Ore, *Ann. Math.*, **36**, 406–437 (1935). We shall use the terminology of G. Birkhoff's paper.

[3] While all right ideals necessarily form a lattice, this is not so in general for the principal ones: The fact that in rings of algebraic integers $\mathfrak{a}$, $\mathfrak{b}$ may be principal ideals while $\mathfrak{a} \cup \mathfrak{b}$ (their "greatest common divisor") is not one, is the origin of Kummer's theory of ideals!

[4] G. Birkhoff, *Ann. Math.*, **37**, 743–748 (1936).

[5] With the usual definitions of $+$ and $\cdot$: $(x_{ij}) + (y_{ij}) = (x_{ij} + y_{ij})$, $(x_{ij}) \cdot (y_{ij}) = \sum_{k=1}^{n} x_{ik}y_{kj}$.