RADICALS AND SUBDIRECT DECOMPOSITIONS

by

Klaus Hoechsmann

B.A., University of British
Columbia, 1957.

Submitted in Partial Fulfillment of the
Requirements of Master of Arts at
McGill University
1958

Signature of Author Klaus Höchsmann

Certified by ______________________

____

ACKNOWLEDGEMENT

The author was holder of a Bursary of the National Research Council of Canada, while this thesis was in preparation. Gratitude is due to that institution for the financial assistance received.

The author is particularly thankful to his supervisor Professor Peck whose kindness and patience were a great encouragement.

TABLE OF CONTENTS

INTRODUCTION

The purpose of this thesis is to state the problem of finding a Wedderburn-Artin structure theorem for semirings. In the now classical case of ring-theory, a certain ideal - called the radical - plays a fundamental role in the development of this theorem. We propose to state in abstract terms what this role is, in order to facilitate a reasonable generalization of the radical-concept for semirings. In order to be useful, any algebraic notion must, of course, possess a characterization which can be formulated in terms of elements in an algebraic structure; the radical satisfies this requirement. In trying to generalize such a notion, we could therefore proceed by studying various generalizations of its intrinsic characterization, and this has indeed been done in the case of rings (Amitsur (1),Divinsky (1)) as well as semirings (Bourne (1)). We shall completely disregard this point of view and produce a radical defined as a homomorphism which maps a given algebraic structure onto a certain composition of presumably well-known structures.

Unfortunately, however, we are yet unable to characterize such a radical internally, except in very few cases, in which it nearly coincides with the old concept.

Nothing in this thesis is essentially new, and source references will be given wherever we are aware of sources. In chapter I, we study abstract algebras in the sense of Birkhoff, and develop our material as far as possible in this abstraction. Chapter II treats ring theory as an example where the outlined method can be carried through completely. Finally, Chapter III is devoted to semirings about which we know little indeed.

It may appear that the paper "On a Wedderburn-Artin Structure Theory of a Potent Semiring" by Bourne & Zassenhaus (1) answers our proposed question. This is not so, since the authors assume the decomposition which we are trying to find, and merely point out its final form. Moreover, as their own example at the end of the note shows, the theorem has very limited application even as it stands.

CHAPTER I

UNIVERSAL ALGEBRA

In order to stress the generality of the method of investigating algebraic structures by decomposition into subdirect unions, we first develop this method as far as feasible in the setting of universal algebra. Most of the details of this chapter can be found in Birkhoff (1). The rest are either well-known or slight generalizations of well-known results.

#1 Subdirect Unions.

By an algebra, we shall mean a set A on which a class (possibly infinite) of functions f_ν of n_ν variables is defined, such that for $x \in A$, $f_\nu(x_1 \ldots x_{n_\nu}) \in A$. Two such algebras are similar if they admit similar operations; i.e., if there exists a one-to-one correspondence between the functions f'_ν on one algebra and the functions f''_ν on the other, the n_ν being the same in both cases. Thus, for example, a commutative group is similar even to a non-commutative one; identities that are satisfied by any of the f_ν are irrelevant. A homomorphism σ on an algebra A is a mapping from A into a similar algebra such that $\sigma(f_\nu(x_1 \ldots x_{n_\nu})) = f_\nu(\sigma(x_1) \ldots \sigma(x_{n_\nu}))$. If this mapping is one-to-one, it is an isomorphism. We shall loosely identify isomorphic algebras.

Now consider a class $\mathfrak{A}$ of similar algebras A_μ, $\mu \in M$, and form the Cartesian product $\prod A_\mu$. $\prod A_\mu$ consists of all functions x from M into $\bigcup A_\mu$, such that $x(\mu) \in A_\mu$. Then, by defining the algebraic operations in $\prod A_\mu$ by letting $f_\nu(x_1 \ldots x_{n_\nu}) = y \in \prod A_\mu$ such that $y(\mu) = f_\nu(x_1(\mu) \ldots x_{n_\nu}(\mu))$, we obtain $\prod A_\mu$ as an algebra similar to all the A_μ. It will be called the <u>direct union</u> of $\{A_\mu\}$.

<u>Proposition 1</u>: Let B be any subalgebra of $\prod(A_\mu)$. Then the <u>projections</u>, $p_\mu: B \to A_\mu$ so that $x \to x(\mu)$, are homomorphisms on B.

<u>Proof</u>: Let $f_\nu(x_1 \ldots x_{n_\nu}) = y \in B$. Then $P_\mu(y) = y(\mu) = f_\nu(x_1(\mu) \ldots x_{n_\nu}(\mu)) = f_\nu(p_\mu(x_1) \ldots P_\mu(x_{n_\nu}))$.

<u>Definition 1</u>: If P_μ maps B <u>onto</u> A_μ for all $\mu \in M$, B is called a <u>subdirect union</u> of the algebras A_μ.

Suppose we are given an algebra A, and, in order to study its structure, we compare it with a class $\mathfrak{A}$ of algebras of known structure. A homomorphism σ on A will then be referred to as an <u>$\mathfrak{A}$-homomorphism</u> if $\sigma(A)$ is isomorphic to some $B \in \mathfrak{A}$.

Theorem 1: A is a subdirect union of $\mathfrak{A}$-algebras if and only if for every pair x,y of distinct elements of A, there exists an $\mathfrak{A}$-homomorphism σ such that $\sigma(x) \neq \sigma(y)$.

Proof: Let $\{\sigma_\mu | \mu \in M\}$ be the totality of $\mathfrak{A}$-homomorphisms on A, and set $\sigma_\mu(A) = A_\mu$. The mapping $\tau : A \to \prod A_\mu$, where $\tau(x) = S$ is such that $s(\mu) = \sigma_\mu(x)$ is obviously a homomorphism of A into $\prod A_\mu$. But if $x \neq y$, there exists a $\mu \in M$ for which $\sigma_\mu(x) \neq \sigma_\mu(y)$ and hence $\tau(x) \neq \tau(y)$. Hence τ is an isomorphism. $\tau(A)$ is a subalgebra of $\prod(A_\mu)$. Consider its projections. If $a \in A_\mu = \sigma_\mu(A)$, there exists an $x \in A$ such that $\sigma_\mu(x) = a$. Therefore if $\tau(x) = S$, $S(\mu) = a$; i.e. $\exists\, S \in \tau(A)$ for which $p_\mu(S) = a$. Hence the projections are onto, and A is isomorphic to a subdirect union.

Conversely, if A is a subdirect union of some of the A_μ, the projections p_μ are $\mathfrak{A}$-homomorphisms and distinguish points of A.

This theorem is fundamental in what is to follow. In order to classify algebras, which are subdirect unions of a certain type of algebra, we must find criteria for existence of enough homomorphisms, whose range is of the desired type, to distinguish points. Further, because of the comparative vagueness of the term "sub-direct union" it is desirable to have conditions for such a union to be <u>the</u> direct union.

We mention, however, one case in which even the notion of subdirect union can give strong results. Suppose that $\mathfrak{A}$ consists of only one algebra A'. Then if A is a subdirect union of $\mathfrak{A}$-algebras, it can be regarded as a set of functions from the index-set M into A'. If A' has a natural topology, M can be topologized so as to make these functions continuous. Then the topology of M, now called the "structure space" of A can give information about the structure of A.

This is, of course, the method underlying Gelfand's representation theory for commutative Banach-algebras.

#2. The Lattice of Homomorphisms.

Definition 1: Let σ be a homomorphism of the algebra A. Then x and y in A are indistinguishable under σ $(x \equiv y(\sigma)$), if $\sigma(x) = \sigma(y)$.

Proposition 1: The relation $x \equiv y(\sigma)$ is a congruence relation; i.e., if $x_i \equiv y_i(\sigma)$ then $f_\nu(x_1 \ldots x_{n_\nu}) \equiv f_\nu(y_1 \ldots y_{n_\nu})$ (σ), for any f_ν.

Proof: If $x_i \equiv y_i$ (σ) then $\sigma(x_i) = \sigma(y_i)$ by definition. Hence $\sigma(f_\nu(x_1 \ldots x_{n_\nu})) = f_\nu(\sigma(x_1) \ldots \sigma(x_{n_\nu})) = f_\nu(\sigma(y_1) \ldots \sigma(y_{n_\nu})) = \sigma(f_\nu(y_1 \ldots y_{n_\nu}))$, and $f_\nu(x_1 \ldots x_{n_\nu})$, $f_\nu(y_1 \ldots y_{n_\nu})$ are indistinguishable under σ.

Definition 2: Let σ, τ be two homomorphisms on A. Then σ is said to be finer than τ ($\sigma \leq \tau$) if for all pairs of elements x,y in A $x \equiv y$ (σ) implies $x \equiv y$ (τ). σ and τ are equal if they are equal as congruence relations; i.e., if $\sigma \leq \tau$ and $\tau \leq \sigma$.

It is clear that σ is finer than τ if and only if it distinguishes at least as many elements as τ . In the future we shall make little distinction between the ideas "homomorphism" and "congruence".

Proposition 2: The class of distinct homomorphisms on A is partially ordered by $\leq$.

Proof: Obviously $\sigma \leq \sigma$. Furthermore, by the difinition of $\leq$, the transitivity of $\leq$ follows from the transitivity of implication.

For the purpose of proving that the homomorphisms on A form a complete lattice we shall note that they have an upper bound and exhibit the infimum of any subset. This will require:

Lemma 1: If P is a partially ordered set with upper bound θ , and if every subset of P has an infimum, then P is a complete lattice.

Proof: Let S be a subset of P and consider the set U of upper bounds of S. Since $\theta \in U$, U has an infimum, which clearly is the supremum of S.

We note that the congruence θ_A , where $x \equiv y$ (θ_A) for *any* pair x,y in A, is an upper bound for all homomorphisms. Incidentally, the congruence ρ_A , where $x \equiv y$ (ρ_A) if and only if $x = y$, is a lower bound. Thus $\rho_A \leq \sigma \leq \theta_A$ for any homomorphism σ on A.

Proposition 3: If H is a set of homomorphisms on A, define $x \equiv y(\varphi)$ to mean that $x \equiv y(\sigma)$ for all $\sigma \in H$. Then φ is a congruence and $\varphi = \inf H$.

Proof: φ is clearly a congruence, because $x_i \equiv y_i$ (σ) for all $\sigma \in H$ implies $f_\nu (x_1 \ldots x_{n_\nu}) \equiv f_\nu (y_1 \ldots y_{n_\nu})$ (σ) for all $\sigma \in H$. $x \equiv y$ (φ) implies $x \equiv y(\sigma)$ for any $\sigma \in H$, so that $\varphi \leq \sigma$. Finally if $\omega \leq \sigma$ for all $\sigma \in H$ then $x \equiv y(\omega)$ implies $x \equiv y(\phi)$ and hence $x \equiv y(\varphi)$, so that $\omega \leq \varphi$. Hence $\varphi = \inf H$.

We can conclude now from lemma 1 and proposition 3, that the homomorphisms form a complete lattice. For the record, we shall also exhibit the form of the supremum.

Proposition 4: Let H be a set of homomorphisms, and let $x \equiv y(\varphi)$ mean that there exists a finite sequence $x = x_1 \ldots x_n = y$, where $x_i \equiv x_{i+1}$ (σ_i) for some $\sigma_i \in H$. Then $\sup H = \varphi$.

Proof: It is easy to see that φ is an equivalence relation, the transitivity following from the fact that the union of two finite sequences is finite.

Now $x_i \equiv y_i(\varphi)$ for $i = 1 \ldots n_\nu$ means that $x_i = x_i^1 \ldots x_i^m = y_i$, where $x_i^j \equiv x_i^{j+1} (\sigma_{ij})$ for some σ_{ij} in H. Obviously these sequences can have the same length m, if elements are repeated when necessary. Let $f_\nu(i,j)$ mean $f_\nu(x_1 \ldots x_i^j \ldots x_{n_\nu})$, and order these lexicographically. Then each member in the resulting sequence of length mn_ν is indistinguishable from the following one under some $\sigma \in H$, and $f_\nu(x_1 \ldots x_{n_\nu}) \equiv f_\nu(y_1 \ldots y_{n_\nu}) (\varphi)$.

Again it is not difficult to see that φ is an upper bound no greater than any other upper bound. Hence $\varphi = \sup H$.

Definition 3: Let an algebra A be given and consider a set $\mathfrak{A}$ of similar algebras. If H is the totality of $\mathfrak{A}$-homomorphisms on A, the $\mathfrak{A}$-radical of A is defined to be $\alpha_A = \inf H$.

We can now restate theorem 1.1 by noting:

Lemma 2: $\alpha_A = \rho_A$ if and only if for any pair x,y of distinct points of A, there exists an $\mathfrak{A}$-homomorphism σ which distinguishes x and y .

Proof: Suppose that $\alpha_A = \rho_A$. Then x,y are indistinguishable under α_A , that is, under all $\mathfrak{A}$-homomorphisms only if they are equal.

Conversely, if x,y are indistinguishable under all $\mathfrak{A}$-homomorphisms only if they are equal, $x \equiv y(\alpha_A)$ implies $x = y$ or $x \equiv y(\rho_A)$. Hence $\alpha_A \leq \rho_A$, and therefore $\alpha_A = \rho_A$.

As a direct consequence we obtain:

Theorem 1: A is a subdirect union of $\mathfrak{A}$-algebras if and only if $\alpha_A = \rho_A$.

Theorem 2: Let $\alpha_A(A) = B$. Then $\alpha_B = \rho_B$.

Proof: We note that, if σ and τ are homomorphisms on A with $\sigma \leq \tau$, then τ induces a homomorphism τ_B on $B = \sigma(A)$, such that for $u = \sigma(x) \in B$, $\tau_B(u) = \tau(x)$. This is single-valued because $\sigma(x) = u = \sigma(y)$ implies that $\tau(x) = \tau(y)$, since $\sigma \leq \tau$.

Now let u,v be distinct points of $B = \alpha_A(A)$; i.e., $u = \alpha_A(x)$ and $v = \alpha_A(y)$, for x,y, in A. There exists an $\mathfrak{A}$-homomorphism σ such that $x \neq y(\sigma)$. Since $\alpha_A \leq \sigma$, σ_B is an $\mathfrak{A}$-homomorphism on B such that $\sigma_B(u) = \sigma(x) \neq \sigma(y) = \sigma_B(v)$. Hence the $\mathfrak{A}$-homomorphisms on B distinguish points and $\alpha_B = \rho_B$ by lemma 2.

Theorem 3: α_A is the finest homomorphism whose range is a subdirect union of $\mathfrak{A}$-algebras.

Proof: Let τ be a homomorphism such that $\tau(A)$ is a subdirect union of $\mathfrak{A}$-algebras A_μ. Then the mappings $p_\mu \tau$: $x \rightarrow \tau(x) = u \rightarrow p_\mu(u)$ are $\mathfrak{A}$-homomorphisms of A, and $\tau = \inf(p_\mu \tau)$. Since α_A is the infimum of all $\mathfrak{A}$-homomorphisms, $\alpha_A \leq \tau$.

If A is not decomposable into a subdirect union, theorems 2 and 3 yield the "least blurred" homomorphic image of A which is decomposable.

#3. Subdirect Irreducibility.

Definition 1: An algebra A is subdirectly irreducible if it is not isomorphic to any subdirect union of algebras other than A itself.

Proposition 1: Let H be the set of all homomorphisms $\sigma \neq \rho_A$ on A. Then A is subdirectly irreducible if and only if inf H $\neq \rho_A$.

Proof: If inf H $= \rho_A$, A is a subdirect union by theorem 2.1 . On the other hand, if A is a subdirect union of A_μ, then the infimum of the projections ρ_μ is already equal to ρ_A . Hence inf H $\neq \rho_A$ is impossible.

Theorem 1: Every algebra A is a subdirect union of subdirectly irreducible algebras.

Proof: For any distinct pair of points x,y in A, we shall exhibit a homomorphism σ , such that $\sigma(x) \neq \sigma(y)$ and $\sigma(A)$ is subdirectly irreducible. Then the theorem follows from theorem 1.1 .

Let H be the set of all homomorphisms on A which distinguish x and y, and consider any totally ordered subset T of H. We prove that $\tau =$ sup T $\in$ H. For if this were not so, $x \equiv y(\tau)$ could be true, and there would exist a finite sequence $x = x_1 \ldots x_n = y$ such that $x_i \equiv x_{i+1}$ (σ_i) for some σ_i in T. But since the σ_i are comparable and finite in number, there would be a greatest among them, say σ_0 , and $x_i \equiv x_{i+1}$ (σ_0) for $i = 1 \ldots n$.

Hence $x \equiv y(\sigma_0)$ which contradicts the hypothesis that $\sigma_0 \in H$.

Since every totally ordered subset of H has an upper bound in H, it follows from Zorn's lemma that H contains a maximal element σ. Obviously $\sigma(x) \neq \sigma(y)$. Now let $B = \sigma(A)$ and consider the two distinct points $u = \sigma(x)$ and $v = \sigma(y)$. If $\varphi \neq \rho_B$ is any homomorphism on B, $\varphi\sigma$ is a homomorphism on A. Since σ is maximal with respect to distinguishing x and y, it follows that $\varphi\sigma(x) = \varphi\sigma(y)$ or $\varphi(u) = \varphi(v)$. Hence B is no subdirect union.

Theorem 3.1, which is due to Birkhoff (2), makes it desirable to study and classify subdirectly irreducible algebras. This has been done to some extent in ring-theory, especially in the case of commutative rings. (cf. McCoy (1)).

#4 Conditions for Finite, Direct Unions.

Definition 1: A partially ordered set P satisfies the descending chain condition (d.c.c.) if any descending chain of distinct elements of P is necessarily finite. Similarly, the ascending chain condition (a.c.c.) is defined.

Theorem 1: Let H be a set of homomorphisms on A, for which $\inf H = \rho_A$, and let P be the totality of infima of subsets of H. Then A is a finite subdirect union of algebras $\sigma_i(A)$ ($\sigma_i \in H$) whenever either the d.c.c. or the a.c.c. holds in P.

Proof: Certainly A is a subdirect union of $\sigma_\mu(A)$ with $\sigma_\mu \in H$. Suppose A is no finite subdirect union of these. Then we can select an infinite sequence $\{\sigma_n\}$ from H by the following rules: (1.) $\sigma_i \ngeq \inf\{\sigma_1 \cdots \sigma_{i-1}\}$. If it became impossible at any stage i to find such a homomorphism, A would already be a subdirect union of $\{\sigma_1 \cdots \sigma_{i-1}\}$, contrary to our assumption. (2.) After obtaining the infinite sequence $\{\sigma_n\}$ satisfying rule 1, we exclude all σ_i for which $\sigma_i \geq \inf\{\sigma_{i+1}, \cdots\}$. This operation does at no stage change $\inf\{\sigma_n\}$. Hence if it were to reduce $\{\sigma_n\}$ to a finite sequence $\{\sigma_1 \cdots \sigma_N\}$, $\inf\{\sigma_1 \cdots \sigma_N\} = \inf\{\sigma_n\}$, so that σ_{N+1} would not have been chosen in the first place because of rule 1. Thus we are left with an infinite sequence $\{\sigma_m\}$ so that $\inf\{\sigma_1 \cdots \sigma_{i-1}\} \nleq \sigma_i \ngeq \inf\{\sigma_{i+1}, \sigma_{i+2} \cdots\}$, for all i.

(a) Suppose P satisfies the d.c.c. Let $H_i = \{\sigma_1 \ldots \sigma_i\}$, and consider the chain $\inf H_1 \geq \inf H_2 \geq \ldots$. The elements of this chain are distinct, since $\inf H_i = \inf H_{i+1}$ implies $\inf\{\inf H_i, \sigma_{i+1}\} = \inf H_i$ or $\sigma_{i+1} \geq \inf H$, which violates the first.rule.

(b) Suppose P satisfies the a.c.c. Let $H_i = \{\sigma_{i+1}, \cdots\}$, and consider the chain $\inf H_1 \leq \inf H_2 \leq \ldots$. Again $\inf H_i \neq \inf H_{i+1}$, this time because of rule (2), and we get an infinite ascending chain.

We have purposely avoided the hypothesis that the chain conditions hold for the partially ordered system of all homomorphisms. This assumption is much too strong in the case of semirings, which have 'many more' homomorphisms than rings.

<u>Definition 2</u>: Two congruences σ, τ are <u>permutable</u> if $\sigma.\tau = \tau\cdot\sigma$, where $x \equiv y(\sigma.\tau)$ means that there exists a z such that $x \equiv z(\sigma)$ and $z \equiv y(\tau)$.

Note that $\sigma.\tau$ is in general not a congruence relation.

<u>Proposition 1</u>: If σ and τ are permutable homomorphisms, $\sigma\cdot\tau = \tau\cdot\sigma = \sup(\sigma,\tau)$. In particular, $\sigma.\tau$ is a congruence.

<u>Proof</u>: $x \equiv y(\sup(\sigma,\tau))$ implies that $x = x_1 \ldots x_n = y$, where $x_i \equiv x_{i+1}$ (σ or τ). Whenever $x_i \equiv x_{i+1}$ (σ), $x_{i+1} \equiv x_{i+2}$ (σ), we can drop x_{i+1} by transitivity. Similarly for repeated τ. Thus we can assume that the congruences connecting x_i and x_{i+1} alternate between σ and τ. But since these are permutable, the whole sequence can be collapsed into three elements as in definition 2. Therefore $\sup(\sigma,\tau) = \sigma\cdot\tau$.

Conversely it is obvious that $x \equiv y(\sigma\cdot\tau)$ implies that $x \equiv y(\sup(\sigma,\tau))$.

Theorem 2: Let H and P be as in theorem 4.1, and suppose that H is finite, i.e., H = $\{\sigma_1 \cdots \sigma_n\}$. Then A is the direct union of the $\sigma_i(A)$, if and only if the elements of P are permutable, and $\sup\{\inf(\sigma_1 \ldots \sigma_i), \sigma_{i+1}\} = \theta_A$ for all $i < n$.

Proof: Let $\sigma_i(A) = A_i$. In order to prove that A is the direct union $\prod A_i$, we must show that for any n-tuple $\{x_i \mid x_i \in A_i, i = 1 \ldots . n\}$, there exists an x in A such that $\sigma_i(x) = x_i$. We proceed by induction.

For x_1 there must be a $z_1 \in A$ so that $\sigma_1(z_1) = X_1$ by definition of subdirect union. Suppose we have found $z_K \in A$ such that $z_K \equiv X_i(\sigma_i)$ for $i \leq k$. Again, we can find a z'_{K+1} so that $\sigma_{K+1}(z'_{K+1}) = x_{K+1}$. Since the elements of P permute, $\theta_A = \inf(\sigma_1 \ldots \sigma_K) \cdot \sigma_{K+1}$. Therefore, since $z_K \equiv z'_{K+1}$ (θ_A), there exists a z_{K+1} such that $z_K \equiv z_{K+1}$ $(\inf(\sigma_1 \ldots \sigma_K))$ and $z_{K+1} \equiv z'_{K+1}$ (σ_{K+1}). Hence $z_{K+1} \equiv x_i(\sigma_i)$ for all $i \leq k+1$.

Conversely, suppose A is the direct union of $A_1 \ldots A_n$. Then it is easily verified that the projections $\sigma_i : A \rightarrow A_i$ satisfy the conditions of the theorem.

#5 Homomorphisms on Semirings.

In this thesis, a semiring S will be an algebraic system with two associative binary operations: addition (+) and multiplication (•), where addition is commutative, and multiplication is left and right distributive over addition.

Further we postulate the existence of an additive identity 0, which also has the property that $0x = x0 = 0$ for all $x \in S$. (Note that this last property of zero is not always assumed in defining a semiring.) If σ is a homomorphism on S, the <u>kernel</u> of σ will be the set of those elements of S which are indistinguishable from zero under σ .

<u>Proposition 1</u>: A subset K of S is the kernel of some homomorphism if and only if

(1) $x, y \in K$ implies that $x+y \in K$.

(2) $x \in K$ implies that ax and xa are in K for any $a \in S$.

(3) $x+y \in K$ and $x \in K$ implies that $y \in K$.

<u>Proof</u>: Let K be the kernel of a homomorphism σ ; i.e., $\sigma(x) = 0$ for all $x \in K$ and for no others. Then

(1) $\sigma(x+y) = \sigma(x) + \sigma(y) = 0 + 0 = 0$

(2) $\sigma(ax) = \sigma(a)\sigma(x) = \sigma(a)0 = 0$ and similarly on the right.

(3) $0 = \sigma(x+y) = \sigma(x) + \sigma(y) = 0 + \sigma(y) = \sigma(y)$.

On the other hand, if K is given with properties (1) to (3), let us define $x \equiv y(\sigma)$ to mean that $x+a = y+b$ for some $a,b \in K$. This is a congruence whose kernel is K. For, let $x_i \equiv y_i \ (\sigma) \ (i = 1,2)$. Then $x_i + a_i = y_i + b_i \ (i = 1,2)$. By summing, $(x_1 + x_2) + (a_1 + a_2) = (y_1 + y_2) + (b_1 + b_2)$; i.e., $x_1 + x_2 \equiv y_1 + y_2 \ (\sigma)$ since $(a_1 + a_2), (b_1 + b_2) \in K$ by (1).

Also, by multiplying, $(x_1 x_2) + (x_1 a_2 + a_1 x_2 + a_1 a_2) = (y_1 y_2) + (y_1 b_2 + b_1 y_2 + b_1 b_2)$ so that $x_1 x_2 \equiv y_1 y_2$ (σ) since the two other terms are in K by (2) and (1). Thus σ is a congruence. Obviously K is indistinguishable from 0 under σ, and further if $x \equiv 0$ (σ) then $x + a = b$ for $a, b \in K$, so that $x \in K$ by (3)

We note that only properties (1) and (2) are needed to construct a congruence. (3) then ensures that all elements congruent zero are in K.

Definition 1: A subset of S is called a semi-ideal if it satisfies properties (1) and (2) above; it is an ideal if it satisfies (3) as well. If I is a semi-ideal, σ as constructed above is called the natural homomorphism associated with I. $\sigma(S)$ is sometimes written S/I, and called the difference-semi-ring of S modulo I.

We shall presently show that the correspondence between homomorphisms and ideals is in general many-to-one. Clearly every homomorphism has only one kernel, but many different homomorphisms might have the same. First some observations of a different nature.

Definition 2: The ring of S is defined as $R(S)=\{x\in S \mid x+y=0 \text{ for some } y\in S\}$. If $R(S)=S$, S is called a ring; if $R(S)=0$, it will be called pure.

The proof that this coincides with the usual definition of "ring" is omitted. Also unproved are the well-known facts concerning the uniqueness of additive inverse and the operation of subtraction in such a system.

Proposition 2: $R(S)$ is an ideal in S, and the difference-semiring modulo $R(S)$ is pure.

Proof: The verification of the first part of this proposition is easy.

Let $x+y\equiv 0 \bmod R(S)$; i.e., $x+y+a=b$ with $a,b\in R(S)$. Since a has an inverse $c\in R(S)$, $x+y=b+c\in R(S)$. Hence, for some $z\in R(S)$, $x+y+z=0$; i.e., $x+(y+z)=y+(x+z)=0$, and $x,y\in R(S)$.

Proposition 3: If R is a ring with a homomorphism σ, $\sigma(x-y)=\sigma(x)-\sigma(y)$ for all $x,y\in R$.

Proof: Since $\sigma(0)+u=u$ for all $u\in\sigma(R)$, we have in particular $\sigma(0)+0=\sigma(0)=0$. Now if $x+y=0$ in R, $\sigma(x)+\sigma(y)=\sigma(0)=0$. Hence $\sigma: y=-x\rightarrow-\sigma(x)$.

Theorem 1: The lattice of homomorphisms on a ring R is isomorphic to the lattice of ideals, where $\inf\{I_\mu\}=\bigcap I_\mu$ and $\sup\{I_\mu\}=\{\Sigma a_i \mid a_i\in I_i$, and the sums are finite$\}$ for ideals.

Proof: Let σ be a homomorphism, K its kernel. It is always true that $x \equiv y$ mod K implies $x \equiv y(\sigma)$, and if R is a ring, the converse holds also, because $\sigma(x) = \sigma(y)$ implies $\sigma(x-y) = 0$ and $x - y \in K$ so that $x \equiv y$ mod K. It follows that ideals and homomorphisms correspond to one another uniquely. The rest of the proof is direct computation. It follows from the form of supremum for ideals that

Corollary: Homomorphisms on a ring are permutable.

Now a counterexample is due to show that this is not generally true in semirings.

Example 1: Let S be a pure semiring without zero divisors (such as the non-negative integers), Then S can be mapped homomorphically onto the lattice (0,I) , where addition and multiplication correspond to taking the supremum and the infimum respectively.

For, let $\tau(x) = I$ if and only if $x \neq 0$ in S'. Then τ is a homomorphism, since $x + y = 0$ implies $x = y = 0$ by purity, and $xy = 0$ implies that either x or y be zero. Its kernel is simply 0; but the isomorphism ρ_S also has this kernel.

τ is what Bourne in (2) calls a "semi-isomorphism", demonstrating that this term is often of little use.

CHAPTER II

THEORY OF RINGS.

As an application of the preceding abstractions, we shall now derive the classical Wedderburn-Artin theorem for "semi-simple" rings. If we dwelt on detail in Chapter I, it was necessary for an intuitive grasp of the point of view taken there; in the sequel we shall omit all standard definitions for the sake of brevity. The material of this chapter is contained explicitly in either Jacobson (1) or Brown and McCoy (1).

It should be noted that theorem 5.1 of chapter I enables us to substitute the notion of ideal for that of homomorphism.

#1 Irreducible Modules.

Definition 1: If A is a ring, M a (right) A-module, the centralizer C(A,M) of M is the ring of module-endomorphisms of M (θ is a module-endomorphism if $\theta(m_1 + m_2) = \theta(m_1) + \theta(m_2)$ and $\theta(ma) = (\theta(m))a$, where $m, m_1, m_2 \in M$ and $a \in A$).

Proposition 1: If M is an irreducible A-module (i.e., contains no proper A-submodule), C(A,M) is a division-ring.

Proof: Let $\theta \in C(A,M)$. It is clear that the kernel of θ, $K(\theta)$, as well as its range, $\theta(M)$, are submodules of M. Since M is irreducible, either (1) $\theta(M) = M$, so that $K(\theta) = 0$ or (2) $\theta(M) = 0$, so that $K(\theta) = M$. In case (2), θ is obviously the zero-endomorphism. In case (1), since $K(\theta) = 0$, and the correspondence between kernels and homomorphisms is unique, θ is an automorphism. θ^{-1} is certainly an automorphism of the additive group of M. Further, $ma = (\theta\theta^{-1}m)a = \theta((\theta^{-1}m)a)$, so that $\theta^{-1}(ma) = (\theta^{-1}m)a$, and $\theta^{-1} \in C(A,M)$.

This proposition or a variant thereof usually goes under the name of Schur's Lemma. It enables us to conclude that M is a vectorspace (free module) over $\Gamma = C(A,M)$ and that, if M is a faithful A-module, A corresponds to a ring of linear transformations on M.

The so-called Density Theorem which follows shows that a certain class of linear transformations on the vectorspace M are <u>always</u> induced by A.

Theorem 1: Let M be an irreducible A-module, Γ its centralizer. Given two finite sequences in M, $\{x_i\}$ and $\{y_i\}$ $(i = 1 \ldots n)$, where the $\{x_i\}$ are linearly independent over Γ, there always is an $a \in A$ such that $x_i a = y_i$.

Proof: For any subset $N \subseteq M$, N^* will mean the annihilator of N in A. Conversely, S^*, for $S \subseteq A$, will be the set of all elements of M annihilated by S.

I. If $N = \sum_{i=1}^{n} \Gamma x_i$, we shall first prove that $(N^*)^* = N$. Obviously $N \subseteq (N^*)^*$ so that it remains to show that $uN^* = 0$ implies $u \in N$, for any $u \in M$.

Let $R \neq 0$ be a right ideal in A, L be Γx (for some arbitrary $x \in M$), and L' the annihilator of L in R. Suppose $uL' = 0$, and define a correspondence $\tau : xR \to uR$ by $\tau(xa) = ua$, for $a \in R$. τ is a function since $x\,a = x\,b$ implies $a - b \in L'$ and $ua = ub$. Since xR, uR are A-submodules of M and hence equal to M, τ maps M into M. It can also be seen that τ is a module-endomorphism; i.e. $\tau \in \Gamma$. Since $\tau(xa) = ua$, $(\tau x - u)a = 0$ for all $a \in R$ and $\tau x - u \in R^*$ so that $u \in R^* + L$.

To prove $(N^*)^* = N$ by induction on n, let $N_K = \sum_{i=1}^{K} \Gamma x_i$. The case $n = 1$ follows directly from the above by setting $R = A$ and $x = x_1$. Suppose we know that $(N_K^*)^* = N_K$. Again we apply the preceding argument, setting $R = N_K^*$ and $x = x_{K+1}$. Suppose $u\,N^*_{K+1} = 0$. Then $uL' = 0$; for if $a \in L'$ then since $a \in R$, it annihilates N_K, and since it also annihilates L, it must be in N^*_{K+1}. Hence $u \in R^* + L$. But by the induction hypothesis $R^* = N_K$ and so $u \in N_{K+1}$.

II. Let M_K be the subspace spanned by $\{x_i \mid i \neq k\}$. Then $x_K \notin M_K = (M^*_K)^*$. Hence some $e_K \in A$ annihilates M_K without annihilating x_K. Thus $x_i e_K = 0$ for $i \neq k$ and $x_K e_K = u_K \neq 0$. Since $u_K A$ cannot be a proper submodule of M, $u_K a_K = y_K$ for some $a_K \in A$. Hence $a = \sum_{K=1}^{n} e_K a_k$ has the property promised in the theorem.

Corollary: If M is an irreducible A-module, finite-dimensional over its centralizer, A induces all linear transformations on M as a vectorspace.

#2 The Jacobson Radical

Aiming at a representation of rings in terms of linear transformations on a vectorspace, we are prompted by the results of section 1 to make the following

Definition 1: A ring A is primitive if there exists a faithful, irreducible A-module. An ideal P in a ring A is primitive if A/P is a primitive ring

Because of the corollary to theorem 1.1 we have already:

Proposition 1: If A is primitive it is isomorphic to a ring of linear transformations.

If $\mathfrak{A}$ is the class of primitive rings, the $\mathfrak{A}$-radical of A can be characterized by its kernel, namely the intersection of all primitive ideals of A. This ideal will be called the Jacobson radical, J(A). Corresponding to theorem I.2.1, we then obtain

Theorem 1: If $J(A) = 0$, A is a subdirect sum of primitive rings.

Before investigating the consequences of this result, we shall give some effective characterizations of J(A).

It turns out that every irreducible A-module can be found as a homomorphic image of A regarded as an A-module (regular representation).

Definition 2: A right ideal $I \subseteq A$ is modular if there exists an $e \in A$ such that $a - ea \in I$ for every $a \in A$. e is called a left identity modulo I.

Proposition 2: M is an irreducible A-module if and only if M is isomorphic to the difference module $A - I$, where I is some modular maximal right ideal.

Proof: If M is an irreducible A-module and $0 \neq x \in M$, $xA = M$. At the same time $xA \simeq A - x^*$ (annihilator of x in A). Now x^* is a modular right ideal since $x \in M$ and hence $x = xe$ for some $e \in A$, so that $x(a - ea) = 0$ and $a - ea \in x^*$ for all $a \in A$. x^* is maximal since the image in $A - x^*$ of any right ideal containing x^* would be a proper sub-module.

Conversely, let $M = A - I$, where I is a modular maximal right ideal. M consists of all cosets $a + I = (e + I)\,a$ (by modularity). So $M = (e + I)A$; also $I = (e+I)^*$. We observe that M contains no submodules because I is maximal. To show that M is not annihilated by all of A(this having been a tacit assumption about modules, so far), we note that $M^* \subseteq (e + I)^* = I$, so that $M^* \neq A$.

Proposition 3: P is a primitive ideal if and only if $P = M^*$, for some irreducible A-module M.

Proof P is primitive only if there exists a faithful irreducible A/P-module M. If we make M into an A-module by setting $ma = m(a+P)$ for $a \in A$, then M is an irreducible A-module and $M^* = P$. On the other hand, if an irreducible A-module M is given, it becomes faithful if converted into an A/P-module, where P is taken as M^*.

Theorem 2: $J(A)$ is the intersection of all modular maximal right ideals of A.

Proof: Let I be a modular maximal right ideal. Then by propositions 2 and 3, $(A-I)^*$ is a primitive ideal. From the proof of proposition 2 it also appears that $(A-I)^* \subseteq I$. Hence $J(A)$, the intersection of all primitive ideals, is contained in the intersection of the modular maximal right ideals I.

Conversely, let P be a primitive ideal. Then $P = M^* = \bigcap x^*$ for all $0 \neq x \in M$. But by the proof of proposition 2, x^* is a modular maximal right ideal. Hence the intersection of all such right ideals is contained in $J(A)$.

With each element $x \in A$ we can associate a minimal modular right ideal $I_x = \{a-xa \mid a \in A\}$ modulo which x is a left identity. It follows easily from Zorn's lemma, that a proper modular right ideal is always contained in a maximal modular right ideal (with the same left identity). Thus whenever I_x is proper, it can be guaranteed that x is excluded from at least one maximal modular right ideal, and hence $x \notin J(A)$.

It follows that $x \in J(A)$ implies that I_x is not proper, i.e., $I_x = A$ (unless $x = 0$). Hence there exists an $a \in A$ such that $a - xa = -x$ or $x + a - xa = 0$. We shall say that such an x is quasi-regular. We can now give a second characterization of $J(A)$:

Theorem 3: $J(A)$ is an ideal in which every element is quasi-regular and which contains all right ideals with that property.

Proof: Let I be a right ideal in which every element is quasi-regular, and let $x \in I$. Suppose $x \notin P = M^*$ for some primitive ideal P. There exists $m \in M$ such that $mx \neq 0$. Hence $(mx)A = M$ and $m(xa) = m$ for some $a \in A$. Since $xa \in I$, we have a y such that $xa + y - (xa)y = 0$, so that $m = m - m0 = m - m(xa + y - xay) = (m - mxa) - (m - mxa)y = 0$ which makes $mx \neq 0$ impossible. Hence $x \in \bigcap P = J(A)$.

#3 The Wedderburn-Artin Theorem.

In order to see more clearly what the structure of primitive rings is, we now restrict ouselves to rings A in which the descending chain condition holds for right ideals. There should be no confusion: although the d.c.c. for two-sided ideals is sufficient to ensure a finite decomposition in case $J(A) = 0$, the present condition is introduced in order to force the structure of each component to be "finite" in some sense.

Proposition 1: If A is primitive, the corresponding A-module M is finite-dimensional over Γ.

Proof: If this were false, we could find an infinite, linearly independent sequence $\{x_n\}$ in M. Let $M_k = \{x_1 \dots x_k\}$ and consider the chain of right ideals $M^*_1 \geqslant M^*_2 \geqslant \dots$ By theorem 1.1, there exists $a_i \in A$ such that $a_i \in M_i$, $a_i \notin M_{i+1}$. Hence the chain is properly descending and thus finite.

Corollary 1: If A is primitive, it is isomorphic to a matrix ring over a division ring.

Proof: It follows from the corollary of theorem 1.1 and some elementary vectorspace theory.

Corollary 2: If A is primitive, it is simple.

Proof: Let $I \neq 0$ be an ideal in A. Then take $0 \neq x \in I$; x corresponds to a non-zero matrix, which by appropriate left and right multiplications and additions can be transformed into the identity matrix e. Hence $e \in I$ and $I = A$.

Theorem 1 (Wedderburn-Artin): If $J(A) = 0$ and A satisfies the d.c.c. for right ideals, then $A = R_1 \oplus \dots \oplus R_n$ is a finite direct sum, where R_i is the ring of all matrices of order m_i over a division-ring.

Conversely, if A has this form, it satisfies the conditions of the theorem.

Proof: By theorems I.2.1 and I.4.1, A is a finite subdirect sum of matrix-rings R_i. To prove the first part of this theorem, we must verify the conditions of theorem I.4.2, where the primitive ideals $P_1 \dots P_n$ take the place of the σ_i. But by corollary 2 above, P_i is maximal (A/P_i being simple), and $(P_1 \cap \dots \cap P_{i-1}) + P_i = A$.

For the converse, we note that the ring A of linear transformations on a vector-space M is always primitive. If $N \subset M$ were an A-submodule, then even $xA = M$ for any $0 \neq x \in N$, so that $M = xA \subseteq N$, which is impossible. Hence M is a faithful, irreducible A-module.

Now it follows, again by theorem I.2.1, that $J(A) = 0$ since A is the direct sum of primitive rings. It remains to prove the d.c.c. Every right ideal I is the direct sum of its components $I_i \subseteq R_i$, which are right ideals in R_i. We can therefore restrict the problem to proving the d.c.c. in a matrix-ring A over a division-ring. It is easily seen that $e_{ii} A$ is a minimal right ideal of A (e_{ii} being a matrix-unit with 1 in position (i,i) and 0 elsewhere) and that $A = e_{11} A \dotplus e_{22} A \dotplus \dots \dotplus e_{mm} A$, if considered as a right A-module, is a direct sum of these. If I is any right ideal of A, then I is the direct sum of some of the $e_{ii} A$. For, $I = A \wedge I = (e_{11} A \wedge I) \dotplus \dots \dotplus (e_{mm} A \cap I)$, where $e_{ii} A \wedge I$ is either 0 or equal to $e_{ii} A$, since it is an ideal contained in the latter. It is obvious now that no descending chain of partial direct sums of the $e_{ii} A$ could be infinite.

The development finishing in this theorem is a complete realization of the plan expounded in chapter I. We defined a class $\mathfrak{A}$ of rings (primitive rings) whose structure is fairly well determined, found a characterization of the $\mathfrak{A}$-radical, and finally obtained a structure theorem in terms of a direct union.

#4 The Radical of Brown and McCoy.

The notion of a primitive ring was conceived as a generalization of a matrix-ring over a division-ring, for a more general form of the Wedderburn-Artin theorem. Another point of view, taken by Brown and McCoy in (1), is to consider simple rings with identity. It must be observed that a simple ring with identity, satisfying the d.c.c. for right ideals, is necessarily a matrix-ring over a division-ring.

Lemma 1: If e is a left identity for a simple ring A, then e is the identity element.

Proof: Since $ex = x$ for all $x \in A$, the set $S = \{ xe - x \mid x \in A \}$ is a two-sided ideal I. If $I = A$, $e = ye - y$ for some $y \in A$, and $x = ex = y(ex-x) = 0$ for all $x \in A$. If $I = 0$, it follows that $xe = x$ for all $x \in A$ and e is a right identity.

Theorem 1: P is a maximal modular (two-sided) ideal in A if and only if A/P is simple and has an identity.

Proof: If P is maximal modular, A/P is simple and has a left identity. Lemma 1, then leads to the desired conclusion.

Conversely, let A/P be simple with identity e, and let τ be the natural homomorphism mapping A onto A/P. Since A/P is simple, P is maximal. Let a be any element such that $\tau(a) = e$. Then, for any $x \in A$, $x - ax \in P$ because $\tau(x - ax) = \tau(x) - e\,\tau(x) = 0$.

If $\mathfrak{A}$ is the class of all simple rings with identity, let the $\mathfrak{A}$-radical of A be called simply the radical, R(A). It follows immediately that:

Theorem 2: R(A) is the intersection of all maximal modular two-sided ideals.

It is obvious now that $J(A) \subseteq R(A)$ because all maximal modular ideals are, in particular, right ideals. The two radicals are generally unequal: if A is the ring of bounded operators on a Hilbert space, $J(A) = 0$ whereas R(A) consists of all completely continuous operators (cf.McCoy (1)).

Again we can give a second characterization. With every $a \in A$ we associate a minimal modular ideal I_a, modulo which a is a left identity, namely the two-sided ideal generated by the set $S = \{x - ax \mid x \in A\}$. We call a pseudo-regular if $I_a = A$.

Theorem 3: R(A) contains only pseudo-regular elements, and every two-sided ideal with that property is contained in R(A).

Proof: Let I be an ideal all of whose elements are pseudo-regular. Take a maximal modular ideal P, and let τ be its natural homomorphism. If $0 \neq x \in I$, where $x \notin P$, then $\tau(x) \neq 0$ and the two-sided principal ideal generated by x will be mapped onto a non-zero ideal $I' \subseteq A/P$. Obviously psuedo-regularity is preserved under homomorphism, and so $I' = A/P$ is composed entirely of pseudo-regular elements.

Of course, the identity e cannot be pseudo-regular, and thus x must be in P.

The Wedderburn-Artin theorem follows as in section 3. However, in this setting we can clarify the role of the d.c.c. in the following:

Theorem 4: If $R(A) = 0$ and A satisfies the d.c.c. for two-sided ideals, then A is a finite direct sum of simple rings with identity element.

Proof: The proof is analogous to that of theorem 3.1. We observe, however, that we do not need the d.c.c. for right ideals to establish the maximality of the kernels of our $\mathfrak{A}$-homomorphisms (in proving that the conditions of theorem I.4.2 hold.)

Now it is clear that the d.c.c. for right ideals is postulated only to make the components of this direct sum into rings of finite matrices.

CHAPTER III.

REMARKS ON SEMIRINGS.

As observed earlier, ideals do not determine homomorphisms in the general case of semirings, and as other methods are yet unavailable, we restrict ourselves to types of semirings in which consideration of ideals can be justified; specifically, to halfrings and distributive lattices. References to various sources will be given throughout the chapter.

#1 General Properties.

To clarify the relation between semi-ideals and ideals, we introduce:

Definition 1: The closure $\overline{I}$ of a semi-ideal I is the smallest ideal containing I (cf. Bourne & Zassenhaus (1)).

Proposition 1: If I is a semi-ideal in a semiring S, then $\overline{I} = \{x \in S \mid x + a = b; a,b \in I\}$.

Proof: Any ideal containing I must contain the set $E = \{x \in S \mid x + a = b;\ a,b \in I\}$ (cf. proposition I.5.1.) Hence we need to prove only that E is an ideal.

If $x+a=b$ and $y+c=d$, then $(x+y)+(a+c) = b+d$; therefore E is closed under addition. If $x+a=b$, then $xy+(ay)=(by)$, and so on. The third ideal property is automatically satisfied by E.

Evidently the definition as well as the proposition apply also to left and right ideals.

Examples: (1) Let p and q be prime numbers and consider the semi-ideals (p) and (q) generated by them in the semiring of non-negative integers Z. $(p)+(q)$ is a semi-ideal properly contained in Z, but $\overline{(p)+(q)}=Z$.

(2) Let I be a semi-ideal in a finite distributive lattice. If $u=\sum_{x\in I} x$ (the notation of addition being substituted for that of union; that of multiplication substituted for that of intersection), then $x\in I$ implies $x\leq u$, and, conversely $x\leq u$ implies $x=xu\in I$. Thus $I=\{x \mid x\leq u\}$. Obviously, $x+a=b$ means that $x\leq b\leq u$ so that $x\in I$. Hence $\overline{I}=I$.

In order to see how "ring-like" a given semiring S is, we consider the Cartesian product $S\times S$ with operations of addition and multiplication defined as follows:

$$(a,b)+(c,d) = (a+c,\ b+d)$$

$$(a,b)\ (c,d) = (ac+bd,\ ad+bc).$$

It is trivial to verify that this is a semiring, A.

Proposition 2: Consider the set $I = \{ x \in A \mid x = (a,a)$ for some $a \in S \}$. I is a semi-ideal, and $R = A/I$ is a ring.

Proof: I is closed under addition. Moreover if $(a,a) \in I$, $(x,y)\,(a,a) = (xa + ya,\ xa + ya) \in I$, and similarly on the right.

R is obviously a semiring. For any $(x,y) \in A$, (y,x) is in A, and $(x,y) + (y,x) = (x+y,\ y+x) \equiv 0$ modulo I. Hence R is closed under subtraction.

S is obviously isomorphic to the subsemiring of A which consists of all pairs of the form $(x,0)$. The natural homomorphism $\tau : A \rightarrow A/I$ thus maps S into the ring R.

Proposition 3: (a) τ is the finest homomorphism from S into a ring.

(b) τ is an isomorphism if and only if S satisfies the cancellation law for addition.

Proof: (a) We observe that $a \equiv b\ (\tau)$ if and only if $a + x = b + x$ for some $x \in S$. For if $a \equiv b(\tau)$, then $(a,0) + (x,x) = (b,0) + (y,y)$ or $(a+x,x) = (b+y,y)$, so that $a + x = b + x$. Conversely, if $a + x = b + x$, $(a,0) + (x,x) = (b,0) + (x,x)$.

Now let σ be any homomorphism from S into a ring P. Then $a \equiv b(\tau)$ implies $a + x = b + x$ and $\sigma(a) + \sigma(x) = \sigma(b) + \sigma(x)$. Since P is a ring, $\sigma(a) = \sigma(b)$. Thus $a \equiv b\ (\sigma)$ and $\tau \leq \sigma$.

(b) If τ is an isomorphism, $a+x=b+x$ (which means $\tau(a)=\tau(b)$) implies $a=b$. Conversely, if the cancellation law holds, $\tau(a)=\tau(b)$ implies $a+x=b+x$, and thus $a=b$.

Corollary: S obeys the cancellation law for addition if and only if it can be embedded in a ring.

Definition 2: If a semiring H can be embedded in a ring, it is called a halfring. The embedding ring H* is the ring of all formal differences of elements of H; more generally, we shall write E* for the formal differences of any subset E of H. If R is a ring, H a halfring such that $R=H^*$, then H is called a generating halfring for R.

#2 The Semi-radical.

One might hope to gain a few ideas about the structure of a semiring by regarding it as the inverse image of a halfring under the natural mapping τ . Just how blurred this image may be, is shown by the example of a lattice L with upper bound I. Here $\tau(L)=0$ is a one-element halfring, because $I+x=I$ for all $x\in L$. However, following Bourne & Zassenhaus (2), we give the

Definition 1: Let $\tau(S)=H$. Then the semi-radical $Z(S)$ is the totality of $x\in S$ such that $\tau(x)\in J(H^*)$.

Proposition 1: Z(S) is a two-sided ideal.

Proof: Let σ be the compound homomorphism $\sigma : S \to H \to H/J(H)$, where $J(H)$ is simply $J(H^*) \cap H$. Clearly $Z(S)$ is the kernel of this homomorphism.

Now we state a description of $Z(S)$ analogous to theorem II.2.3:

Theorem 1: $Z(S)$ is the maximal right ideal I of S, such that for $x_1, x_2 \in I$ there exist y_1, y_2 in S for which $x_1 + y_1 + x_1 y_1 + x_2 y_2 = x_2 + y_2 + x_2 y_1 + x_1 y_2$.

Proof: Notice that this relation is just a translation of the idea of quasi-regularity into semiring language.

Writing $x' = \tau(x)$, we note that for every pair $x_1, x_2 \in Z(S)$, $(x'_1 - x'_2) \in J(H^*)$ is quasi-regular. This means that there exist $Z_1, Z_2 \in S$, such that $(x'_1 - x'_2) + (Z'_1 - Z'_2) + (x'_1 - x'_2)(Z'_1 - Z'_2) = 0$ (in H^*), or $x'_1 + Z'_1 + x'_1 Z'_1 + x'_2 Z'_2 = x'_2 + Z'_2 + x'_2 Z'_1 + x'_1 Z'_2$, or $\tau(x_1 + Z_1 + x_1 Z_1 + x_2 Z_2) = \tau(x_2 + Z_2 + x_2 Z_1 + x_1 Z_2)$; implying that for some $y \in S$, $x_1 + Z_1 + x_1 Z_1 + x_2 Z_2 + y = x_2 + Z_2 + x_2 Z_1 + x_1 Z_2 + y$. Adding $x_1 y + x_2 y$ to both sides of the last relation, we obtain the one stated in the theorem by setting $y_1 = Z_1 + y$, $y_2 = Z_2 + y$.

Conversely, let I be a right ideal with the property in question. We must prove that $(\tau(I))^* \subseteq J(H^*)$, for which it suffices to show that in $(\tau(I))^*$ every element is quasi-regular.

This is easily checked by following the above argument backward.

In the next section we shall study those semirings to which this notion of radical is strictly applicable.

#3 Structure of Halfrings.

Although halfrings are known to be subsets of rings, it is of interest to ask what part of the ring-structure is made up of the generating halfring. The present section is devoted to this question.

Proposition 1: Let H be a halfring, I a semi-ideal in H. Then I^* is an ideal in H^* and $I^* \cap H = \bar{I}$.

Proof: Since I^* is the collection of all differences of elements of I, it is closed under subtraction as well as under multiplication by differences of elements in H. Hence I^* is an ideal. Further $I^* \cap H = \{x \in H \mid x = a - b;\ a,b \in I\} = \{x \in H \mid x+b = a;\ a,b \in I\} = \bar{I}$.

Clearly, proposition 1 applies to left, right, or two-sided ideals. In the following proposition we shall mean by the word "ideal" any one of these three classes.

Proposition 2: Let L^* be the lattice of ideals of H^*, L that of H. Then $L^* \simeq L$ under the correspondences $I^* \leftrightarrow I = I^* \cap H$.

Proof: By proposition 1, the indicated correspondence is one-to-one. To verify that it is an isomorphism, we observe:

$$(1)\ \bigcap I^*_\mu \to \bigcap I^*_\mu \cap H = \bigcap (I^*_\mu \cap H) = \bigcap I_\mu .$$

$$\begin{aligned}(2)\ \bigcup I^*_\mu = \Sigma I^*_\mu \to (\Sigma I^*_\mu) \cap H &= \{x \in H \mid x = x_1 + \dots + x_n ,\ x_i \in I^*_{\mu_i}\} \\ &= \{x \in H \mid x = (a_1 - b_1) + \dots + (a_n - b_n), \\ &\qquad\qquad a_i, b_i \in I_{\mu_i}\} \\ &= \{x \in H \mid x + (b_1 + \dots + b_n) = a_1 + \dots + a_n\} \\ &= \overline{\Sigma \; I_\mu} = \bigcup I_\mu .\end{aligned}$$

It follows now that decomposition of halfrings can be studied in the same way as that of rings, provided that the $\mathfrak{a}$-homomorphisms are natural homomorphisms of ideals. In particular:

Theorem 1: If a halfring H has zero semi-radical and satisfies the d.c.c. for right ideals, then $H = H_1 \oplus \dots \oplus H_n$, where H_i is a generating half-ring of a matrix-ring over a division-ring.

Proof: If H has zero semi-radical, then $J(H^*) = 0$. Also, since for any right ideal $R^* \subseteq H^*$, $R = R^* \cap H$ is a right ideal in H, H* satisfies the d.c.c. Hence $H^* = H^*_1 \oplus \dots \oplus H^*_n$, where H^*_i is a matrix-ring over a division-ring, and $H = H_1 \oplus \dots \oplus H_n$, where $H_i = H^*_i \cap H$.

It remains to investigate generating halfrings H_i of matrix rings. Now H^*_i is a simple ring, and hence so is H_i by proposition 2. Since the ring of H_i is an ideal in H_i (proposition I.5.2), there appear only two cases:

(1) H_i is a ring. Then $H_i = H^*_i$ and thus its structure is determined.

(2) H_i is pure. This raises difficult questions, which we shall discuss, though not answer, in the remainder of this section.

Proposition 3: Let H be a pure generating halfring of a ring R. Then H is contained in a *maximal* pure generating halfring (m.p.g.h.)

Proof: Consider the set S of all pure generating halfrings containing H, partially ordered by inclusion. If T is any totally ordered subset, its union is a pure generating halfring. The proposition therefore follows from Zorn's lemma.

We shall denote the half-ring of left operators (cf. Bourne & Zassenhaus (1)) of a halfring H by H_L .

Lemma 1: If H is an m.p.g.h., $H^* \cap H_L = H$.

Proof: Certainly $H \subseteq H_L \cap H^*$, thus leaving us to prove only that $H_L \cap H^*$ is pure. If $\theta, \varphi \in H_L$, $\theta + \varphi = 0$ implies $\varphi(x) + \theta(x) = 0$ and hence $\varphi(x) = \theta(x) = 0$ for all $x \in H$. Therefore $\varphi = \theta = 0$.

Theorem 2: If H is a pure generating halfring of a matrix-ring over a division-ring D, D must be of characteristic zero.

Proof: By proposition 3, H* contains an m.p.g.h. H'. The identity of H*, $e \in H^* \wedge H'_L = H'$. Hence $ne = 0$ for all n, since H' is pure. It is therefore necessary only to study matrix-rings over division-rings of characteristic zero.

In the field R of rational numbers any set of the form $S = \{ x \in R \mid x \geqslant r \geqslant 0 \}$ is a pure generating halfring. However, there is only one m.p.g.h., namely the halfring of non-negative rationals. Suppose a halfring $H \subseteq R$ contains a negative number $-p/q$. (p,q being natural numbers). Then $pq\ (-p/q) \in H$; ie., $-p^2 \in H$. But $(-p/q)^2 = p^2/q^2$, and thus $p^2 \in H$. Hence H is not pure. In general, the question of what m.p.g.h.'s are contained in an arbitrary division ring is not so easily answered.

Now let M be the ring of all n by n matrices over R, and consider the subset H consisting of the zero matrix plus all matrices with positive entries. H is a pure generating halfring of M, but is not maximal. We conclude this section by stating the conjecture that if H is an m.p.g.h. of a matrix-ring over a division-ring D, then (with perhaps some minor additional assumption) H is the set of all matrices with entries in a generating halfring of D. This, unfortunately, we are unable to prove, although no counterexample seems available.

#4 Distributive Lattices.

A distributive lattice is obviously a semiring in which the product of two elements is simply their infimum, the sum their supremum. We shall investigate such lattices by studying the homomorphisms induced by maximal ideals.

Let L be the given lattice, and henceforth suppose that L has a lower bound 0 and an upper bound I.

Lemma 1: If M is a maximal ideal in L, L/M $\simeq$ (0,I), the lattice of two elements.

Proof: L/M has to be simple since M is maximal. But if L/M contained a third element a , then $\{x \mid x \leq a\}$ would be an ideal.

If α_L is the infimum of all homomorphisms on L induced by maximal ideals, then, by the results of chapter I, L is a semiring of functions from $\mathfrak{M}$, the set of maximal ideals, into (0,I), provided that $\alpha_L = \rho_L$. If $\alpha_L = \rho_L$, we shall call L a reduced lattice.

Theorem 1: A reduced lattice L is isomorphic with a semiring of subsets of the collection of its maximal ideals, $\mathfrak{M}$.

Proof: We have remarked that L is a class of functions from $\mathfrak{M}$ into (0,I). With each such function f we associate the subset of $\mathfrak{M}$ on which f(x) = I, and observe that the pointwise addition and multiplication of these functions corresponds precisely to the unions and intersections of the respective sets.

Proposition 1: If $x \equiv I$ (α_L), then $x = I$.

Proof: If $x \neq I$, the set $\{ z \in L \mid z \leq x \}$ is an ideal in L, which is easily seen (Zorn's lemma) to be contained in some maximal ideal M. Hence $x \equiv 0 (\text{mod } M)$.

Proposition 2: A lattice L is reduced if and only if for any pair $x, y \in L$, the relation $x = y$ is equivalent to

(*) $z + x = I$ implies $z + y = I$, for all $z \in L$.

Proof: Since $x = y$ always implies (*), we need only prove that (*) implies $x = y$.

If L is reduced and (*) holds, then (*) holds among the components of x,y, and z in every $L/M \simeq (0,I)$ where it implies that $x \equiv y$ (mod M). Since L is reduced, this means that $x = y$.

Conversely, suppose L is not reduced. Then there exists a pair $x, y \in L$ such that $x \neq y$ but $x \equiv y (\text{mod } M)$ for all $M \in \mathfrak{M}$. Thus for every M, $x + z = y + z (\text{mod } M)$. If $x + z = I$, $y + z \equiv I (\text{mod } M)$ for all M, and hence $y + z = I$ by proposition 1.

We are now able to derive a form of Stone's theorem. It will be recalled that a Boolean algebra is a complemented distributive lattice with 0 and I, and that complements are unique.

Theorem 2: Every Boolean algebra is isomorphic to a field of subsets of a set.

Proof: We should remark that by a "field" a system of sets is meant, which is closed under union, intersection, and complementation.

The theorem follows at once from theorem 1, if we observe that a Boolean algebra satisfies the condition of proposition 2 and hence is a reduced lattice.

The foregoing is a drastic specialization of the treatment of "positive semirings" given by Słowikowski and Zawadowski in (1). In that paper, which touches on the present subject only incidentally, the authors also define the "radical" to be the intersection of all maximal ideals. We wish to point out that this radical is not an $\mathfrak{a}$-radical in our sense except in the case of reduced lattices. Neither is it a special case of the semi-radical defined in section 2, for any distributive lattice with identity I contains proper maximal ideals while the semi-radical is clearly the whole lattice since $x + I = y + I$ for any x,y in the lattice.

BIBLIOGRAPHY

S.A. Amitsur (1), A General Theory of Radicals I, Amer. J. Math., vol.74, 774-786, 1952.

G. Birkhoff (1), Lattice Theory, 2nd edition, Amer. Math. Soc., New York, 1948. (2) Sub-direct Unions in Universal Algebra, Bull. Amer. Math. Soc., vol.50, 764-768, 1944.

S. Bourne (1), The Jacobson Radical of a Semiring, Proc. Nat. Ac.Sc., vol. 37,163-170, 1951. (2), On the Homomorphism Theorem for Semi-rings, Proc. Nat. Ac.Sc., vol. 38, 118-119, 1952.

S. Bourne & H. Zassenhaus (1), On a Wedderburn-Artin Structure Theory of a Potent Semiring, Proc.Nat. Ac.Sc.,vol.43,613-615, 1957. (2), On the Semiradical of a semiring, unpublished.

B.Brown & N.McCoy (1), Radicals and Subdirect Sums, Amer. J.Math., vol.69, 46-58, 1947.

N. Divinsky (1), Pseudo-regularity, Can.J.Math.vol.7, 401-410, 1955.

N. Jacobson (1), Structure of Rings, Amer. Math. Soc., Providence, R.I., 1956.

N. McCoy (1), Subdirect Sums in Rings, Bull. Amer. Math. Soc., vol. 53, 856-877, 1947.