FAIN, Charles Gilbert, 1932-
SOME STRUCTURE THEOREMS FOR NEARRINGS.

The University of Oklahoma, Ph.D., 1968
Mathematics

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

SOME STRUCTURE THEOREMS FOR NEARRINGS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

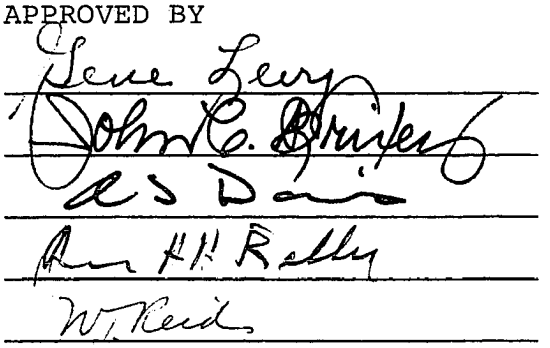
CHARLES GILBERT FAIN

Norman, Oklahoma

1968

SOME STRUCTURE THEOREMS FOR NEARRINGS

APPROVED BY



DISSERTATION COMMITTEE

ACKNOWLEDGMENT

The author deeply appreciates the suggestions and criticisms of the members of the Dissertation Committee, and gratefully acknowledges the unfailing encouragement and advice of Dr. Gene Levy, under whose direction this dissertation was prepared.

TABLE OF CONTENTS

SOME STRUCTURE THEOREMS FOR NEARRINGS

CHAPTER I

INTRODUCTION

Studies of the ring of endomorphisms of an abelian group and the ring of linear transformations of a vector space lead naturally to investigation of the set of endomorphisms of an arbitrary group and the set of affine transformations of a vector space. These latter sets do not form rings under the "natural" operations of addition and multiplication, that is, pointwise addition and composition of mappings. The set of all mappings of an arbitrary group into itself, together with those natural operations, does form a more general algebraic system called a nearring. The set of endomorphisms determines a particularly tractable subnearring of this system, and the set of affine transformations of a vector space also forms a nearring.

A nearring is an algebraic system that satisfies the axioms of a ring with the possible exceptions of the commutative law of addition and one of the distributive laws. In this paper only left nearrings will be considered; that is, the right distributive law is <u>not</u> assumed as an axiom.

With the obvious changes of "left" to "right", any statement that is valid for left nearrings is also valid for right nearrings.

Nearfields, those nearrings in which the multiplicative semigroup of nonzero elements is a group, were introduced by Dickson [8] in 1905. Further studies of nearfields were published in 1936 by Zassenhaus [17], and in 1940 by Kalscheuer [10] and B. H. Neumann [15]. However, the study of nearrings, the natural generalization of nearfields, dates only from Blackett's article [6] in 1953 on the structure of certain "semisimple" nearrings. Betsch [5] in 1954 extended the definition of the Jacobson radical of a ring to those nearrings considered by Blackett in his paper of the preceding year and showed that such a nearring is semisimple (as defined by Blackett without the use of a radical) if and only if its Jacobson radical is zero. In the past fifteen years other radicals and radical-like structures have been studied for several important classes of nearrings. (See [2], [7], [12], [13], [16].)

In this paper some structure theorems are established for general nearrings and for the "special" nearrings considered by Blackett and Betsch. Objects of particular interest in this regard are the Jacobson radical, primitive nearrings, and nearfields. Chapter II gives basic definitions, some results of Blackett and Betsch, and extends the Betsch definition of the Jacobson radical to general

nearrings. Chapter III restates for nearrings the standard theory of subdirect sum decomposition of rings into subdirectly irreducible and primitive component rings. In Chapter IV various properties of nearrings, primitive nearrings, and the radical are established. In Chapter V the decomposition theory of Chapter III is applied to identify those nearrings that have representations as subdirect sums of nearfields. A different approach to the structure of nearrings, a Peirce decomposition, is given in Chapter VI.

The results in this paper, especially those in Chapters IV and V, that are not specifically attributed to others are the work of the author. Many theorems of ring theory are extended here to nearrings; most of these may be found in the books by Jacobson [9] and McCoy [14].

It should be pointed out that, in many instances, the standard proofs from ring theory could not be adapted to nearrings, because of the extensive use made of the concept of quasi-regularity in the Jacobson structure theory for rings. Quasi-regularity is closely related to the arithmetic of elements, but in general nearrings this arithmetic is severely limited by the assumption of only one distributive law. In the literature, (e.g., [3] and [12]), quasi-regularity has been of limited utility even in restricted classes of nearrings.

CHAPTER II

THE JACOBSON RADICAL OF A NEARRING

A general (left) nearring is an ordered triple $(N,+,\cdot)$, where N is a nonempty set and + and $\cdot$ are binary compositions (called addition and multiplication, respectively) on N such that

(1) $(N,+)$ is a group (not necessarily commutative)

(2) $(N,\cdot)$ is a semigroup

(3) multiplication is distributive, from the left, over addition. The multiplication sign is usually omitted, multiplication being indicated by juxtaposition of symbols. Condition (3), the left distributive law, may thus be expressed by $r(s + t) = rs + rt$ for all r, s, and t in N.

A special (left) nearring, (called a C-ring by Berman and Silverman [4]), is a general nearring in which $0n = 0$ for each n in N. Here, 0 is the identity element of $(N,+)$. The symbol N will be used for a nearring, general or special. When not otherwise specified, N is understood to be a general nearring. Of the examples cited in Chapter I, the set of all transformations of an arbitrary group into itself is a general nearring if the group has more than one

element, as is the set of all affine transformations on a vector space of more than one element. The subnearring of group transformations determined by the endomorphisms is a special nearring. A nearfield is also a special nearring. (See Theorem 5.1.) Of course, any ring is a special nearring, and any division ring is a nearfield.

Betsch defined the Jacobson radical only for special nearrings. However, his definitions and results are valid with almost no alteration for general nearrings and they will be so stated here. Most of the definitions and, with the exception of Theorems 2.1 and 2.8, all theorems stated formally in this chapter are from the paper [5] by Betsch.

A not necessarily commutative group $(G,+)$ is called a (right) N-group if there is defined a right multiplication of the elements of G by the elements of N, the products being again in G, such that $g(m + n) = gm + gn$ and $g(mn) = (gm)n$ for each g in G and every m and n in N. N-groups do exist; $(N,+)$ with its nearring multiplication is an N-group. In any nearring, the left distributive law implies $n0 = 0$ for each n in N, and similarly $g0_N = 0_G$ for each g in any N-group G. (Subscripts will be used, when necessary, to distinguish between the zero of a nearring N and the zero of an N-group G.) It is not generally true, however, that $0_N n = 0_N$. For example, on any nonzero additive group, the zero map followed by a map that takes zero onto a nonzero element does not have the same result as the zero map alone.

Thus not every nearring is special. Indeed, a simple argument yields

Theorem 2.1: $0_G n = 0_G$ for each n in N and each N-group (G,+) if and only if N is a special nearring.

Proof: Assume N is special. Since $0_G 0_N = 0_G$, it follows that

$$0_G n = (0_G 0_N)n = 0_G(0_N n) = 0_G 0_N = 0_G$$

for each n in N. Since (N,+) is itself an N-group, the converse is obvious.

A subgroup H of an N-group G for which $HN = \{hn \mid h \in H, n \in N\} \subseteq H$ is called an N-subgroup of G. Clearly, an N-subgroup of an N-group is itself an N-group. The N-subgroups of (N,+) are called N-modules. An N-module M is invariant if $NM \subseteq M$. A nonzero N-group G is minimal if it has no proper nonzero N-subgroups; G is essentially minimal if it is minimal and $GN \neq \{0\}$. An N-homomorphism f of an N-group G into another N-group is a group homomorphism f such that $(gn)f = (gf)n$ for each g in G and n in N.

For examples of some of these concepts, let N be a ring. Clearly, any ring module of N is an N-group, any ideal of N is an invariant N-module, and any ring module homomorphism is an N-homomorphism. Betsch [5] showed that when N is a ring the essentially minimal N-groups coincide with the irreducible ring modules of N.

A mapping f of a nearring N into another nearring is

a nearring homomorphism if $(m + n)f = mf + nf$ and $(mn)f = (mf)(nf)$ for each m and n in N. The usual elementary argument shows that the image of a nearring under a nearring homomorphism is again a nearring. The kernels of nearring homomorphisms are called ideals. Blackett [6] showed that K is an ideal of N if and only if K is a normal subgroup of (N,+) that satisfies

(1) $NK \subseteq K$ and

(2) $(m + k)n - mn$ is in K for each k in K and m and n in N.

Normal subgroups of (N,+) that satisfy (1) above are called left ideals; those that satisfy (2) are called right ideals. Blackett also showed in [6] that the right ideals of N are just the kernels of N-homomorphisms of the N-group (N,+). In a special nearring each right ideal K is an N-module, because $kn = (0 + k)n - 0n$ is in K for each k in K and n in N. Hence each ideal K is an invariant N-module if N is special. In a general nearring, however, KN may not be contained in K. With the usual definitions of coset addition and multiplication, the cosets of an ideal K in the nearring N form the difference nearring N/K.

The elements n in N such that $gn = 0$ for a fixed g in an N-group G form a right ideal A_g of N, the annihilator right ideal of g; the elements n in N such that $gn = 0$ for all g in a fixed N-group G form an ideal A_G of N, the annihilator ideal of G. A_G is just the intersection of the A_g for all elements g in G.

The intersection of the annihilator ideals of all minimal N-groups is called the (Jacobson) radical of N. It follows that if there is no minimal N-group, the radical is N itself. The radical J of N is easily seen to be the intersection of the annihilator ideals of only the essentially minimal N-groups. Again, if there is no essentially minimal N-group, J is equal to N. Because the intersection of ideals is an ideal, J is an ideal of N.

Theorem 2.2: If N is a ring, the essentially minimal N-groups coincide with the irreducible right ring modules of N, and the nearring radical of N coincides with the Jacobson radical of the ring N.

The set {0} is an ideal in any nearring. As an ideal {0} will be written (0). The ideal (0) is an N-module if and only if N is special.

Theorem 2.3: If J is the radical of the nearring N, the radical of the difference nearring N/J is the zero ideal.

Theorem 2.4: If K is an ideal of N, J the radical of N, and I the radical of N/K, then $Jf \subseteq I$, where f is the natural map of N onto N/K.

A nearring N is called primitive if there exists an essentially minimal N-group G such that the annihilator ideal A_G is the zero ideal. It is immediate from the definitions that the radical of a primitive nearring is the zero ideal. An ideal P of N is called primitive if N/P is a primitive nearring.

Lemma 2.5: An ideal P of a nearring N is primitive if and only if P is A_G for some essentially minimal N-group G.

Theorem 2.6: The radical of a nearring N is the intersection of the primitive ideals of N.

A proper (nonzero) right ideal K of a nearring N is called module-maximal (module-minimal) or m-maximal (m-minimal) if there exists no N-module A such that $K \subset A \subset N$ ($(0) \subset A \subset K$). Here the symbol $\subset$ implies strict inclusion. In a general nearring, an m-maximal (m-minimal) right ideal may not be maximal (minimal) as a right ideal, because there may be right ideals that are not modules (e.g., the ideal (0) in a nearring that is not special). In a special nearring, no such confusion arises.

A proper right ideal K of a nearring N is called modular if there is an element e in N such that n - en is in K for each n in N. Such an element e is called a left identity modulo K. If K is a modular ideal, N/K has (e + K) as a left identity.

Theorem 2.7: If G is an essentially minimal N-group, there is an element g in G such that gN = G and A_g is a modular m-maximal right ideal of N. Conversely, if K is a modular m-maximal right ideal of N, then there exists an element g in an essentially minimal N-group G, such that gN = G and $A_g = K$.

In the above theorem, G is actually N-isomorphic to the difference N-group $(N,+) - (A_g,+)$. A direct proof of

this is not difficult. However, the isomorphism is a consequence of Theorem 2.7 and

Theorem 2.8: If G is an N-group and gM = G for some g in G and some N-module M, then G is N-isomorphic to the difference N-group $(M,+) - (A\cap M,+)$, where A is the annihilator right ideal (usually written A_g) of the element g.

Proof: The annihilator A is a right ideal of N, so (A,+) is a normal subgroup of (N,+). Hence $(A\cap M,+)$ is a normal subgroup of (M,+), so the difference group $\overline{M} = (M,+) - (A\cap M,+)$ exists. The right ideal property of A is used to show that the multiplication in $\overline{M}$ by elements of N given by $\overline{m}n = \overline{mn}$ is well-defined. Indeed, let $\overline{m}_1 = \overline{m}_2$ in $\overline{M}$. Then $-m_1 + m_2$ is in $A\cap M$, and if follows that

$$m_2n - m_1n = (m_1 + (-m_1 + m_2))n - m_1n$$

is in $A\cap M$ for each n in N, and hence that $\overline{m_1n} = \overline{m_2n}$. Finally, it is easily verified that the map f from G = gM to $\overline{M}$ given by $(gm)f = \overline{m}$ is an N-isomorphism.

The radical of a nearring N is the intersection of the annihilator ideals of all essentially minimal N-groups, and each such annihilator ideal is the intersection of the annihilator right ideals of the elements of its essentially minimal N-group. By Theorem 2.7, the set of annihilator right ideals of such elements coincides with the set of modular m-maximal right ideals of N. There follows then

Theorem 2.9: The radical of a nearring N is the inter-

section of the modular m-maximal right ideals of N.

A nearring N will be called semisimple if its radical is the zero ideal; N will be called radical if its radical is N itself. A nearring N satisfies the minimum condition if each nonempty collection of nonzero N-modules contains a minimal N-module. An N-module M is said to be nilpotent if there is a positive integer k, such that the product of k arbitrary elements of M is always zero; M^k will represent the set of all such k-fold products of elements of M. An N-module M is said to be nil if each element of M is nilpotent.

Theorem 2.10: In a special nearring N with minimum condition, {0} is the only nilpotent N-module if and only if N is semisimple.

It was in order to obtain this theorem that Betsch defined the nearring radical. Blackett [6] had investigated the structure of semisimple special nearrings with minimum condition. His definition of semisimple was made, however, without use of the concept of a radical. He defined a class of simple nearrings, and showed that a special nearring N with minimum condition is simple if and only if N is semisimple and all essentially minimal N-groups are N-isomorphic. He also proved that if a semisimple special nearring N with minimum condition has more than one element, then N is a finite direct sum of certain ideals of N, each of which is simple when it is considered as a nearring.

The Betsch definition of the radical was extended by Beidleman in 1965 [2] to the radical of any N-group, where N is a special nearring. Many of the results in Chapter IV could be reformulated in terms of this N-group radical, or rather in terms of its generalization for general nearrings.

CHAPTER III

SUBDIRECT SUMS OF NEARRINGS

The theory of subdirect sum representation of rings carries over almost word for word to nearrings. The discussion below follows McCoy [14].

Let N_i be a collection of nearrings indexed by the elements of a set I and let S be the set of all mappings f from I into the union of the N_i such that $(i)f$ is in N_i for each i in I. If addition and multiplication are defined in S by

$$(i)(f + g) = (i)f + (i)g \text{ and } (i)(fg) = ((i)f)((i)g),$$

then S becomes a nearring, the complete direct sum of the N_i. S is a special nearring if and only if each N_i is a special nearring. The subset S' of S consisting of those functions in S whose value at i is 0_i (the zero of N_i) for all but a finite number of i in I is a subnearring of S. This subnearring S' is the discrete direct sum of the N_i.

With each i in I there is associated the evaluation map h_i from S into N_i which takes each f into $(i)f$. Clearly, from the definitions of addition and multiplication in S, each h_i is a nearring homomorphism. Hence, if T is any

subnearring of S, then $(T)h_i$ is a subnearring of N_i. A subnearring T of the complete direct sum is a subdirect sum of the components N_i of S if $(T)h_i = N_i$ for each i in I. A nearring N has a representation as a subdirect sum of the nearrings N_i if there exists an isomorphism of N with some subdirect sum of the N_i.

Theorem 3.1: A nearring N has a representation as a subdirect sum of the nearrings N_i if and only if for each i in I there exists a homomorphism p_i of N onto N_i, and each nonzero element of N has a nonzero image under some p_i.

Proof: If T is a representation of N as a subdirect sum of the components N_i, let h be an isomorphism of N onto T, and let h_i be the natural homomorphism of T onto N_i for each i in I. Then any nonzero n in N has a nonzero image nh under the isomorphism h and hence for some i in I, $0 \neq (nh)h_i = n(hh_i)$. The composite map hh_i is the required homomorphism p_i.

Conversely, if $\{p_i | i \in I\}$ is such a family of homomorphisms, then for each n in N the map f_n from I to the union of the N_i defined by $(i)f_n = (n)p_i$ is in the direct sum S of the components N_i. Since each p_i is a homomorphism, the map P from N into S defined by $(n)P = f_n$ is a homomorphism. Now, for each nonzero n in N there is some p_i such that $0 \neq (n)p_i = (i)f_n$, so f_n is the zero of S if and only if $n = 0$. Thus the kernel of P is $\{0\}$, so P is one-to-one, and (N)P is an isomorphic image of N. Finally, (N)P is

indeed a subdirect sum, since $Np_i = N_i$ by hypothesis, and $(nP)h_i = (f_n)h_i = (i)f_n = (n)p_i$ for each n in N. Thus $(NP)h_i = Np_i = N_i$.

Since the kernels K_i of the homomorphisms p_i of this theorem are ideals of N, it follows from the Fundamental Homomorphism Theorem (which holds by the very definition of nearring ideals) that Theorem 3.1 can be restated as

Corollary 3.2: A nearring N has a representation as a subdirect sum of nearrings N_i if and only if for each i in I there is an ideal K_i of N such that N/K_i is isomorphic to N_i and the intersection of all the K_i is the zero ideal.

From Theorem 3.1 it is clear that any set of homomorphic images of N which contains one or more isomorphic images of N can serve as the set of components in a subdirect sum representation of N. Such a representation is called trivial. A nearring is subdirectly irreducible if it has no nontrivial representation as a subdirect sum. That is, N is subdirectly irreducible if each subdirect sum representation includes among the components an isomorphic copy of N.

It follows from Corollary 3.2 that N has a nontrivial subdirect sum representation if and only if there is a family $\{K_i\}$ of nonzero ideals of N whose intersection is the zero ideal. Hence

Corollary 3.3: A nonzero nearring N is subdirectly

irreducible if and only if the intersection of all the nonzero ideals of N is nonzero. Equivalently, $N \neq \{0\}$ is subdirectly irreducible if and only if there is a (necessarily unique and minimal) nonzero ideal of N that is contained in each nonzero ideal of N.

With the aid of Corollaries 3.2 and 3.3 it can now be shown that the subdirectly irreducible nearrings are "universal components" in the sense that every nearring has a representation among the subdirect sums of such components.

Theorem 3.4: Each nearring N is isomorphic to a subdirect sum of subdirectly irreducible nearrings.

Proof: The one-element nearring $N = \{0\}$ is clearly subdirectly irreducible. If there is a nonzero element n in N, consider the set Z of all the ideals K of N that do not contain n. Certainly Z is nonempty since it contains the zero ideal. The hypotheses of Zorn's Lemma are satisfied by Z with the partial ordering of set inclusion, so there is a maximal element K_n in Z. Thus n is an element of any ideal I of N that properly contains K_n. Consider now N/K_n and the natural homomorphism h of N onto N/K_n. Any nonzero ideal L of N/K_n has as preimage the ideal Lh^{-1} of N which properly contains K_n. Hence Lh^{-1} contains n, so $\overline{0} = K_n \neq nh$, and nh is in each nonzero ideal L of N/K_n. By Corollary 3.3, N/K_n is subdirectly irreducible.

The construction of K_n can be repeated for each nonzero n in N. Since each n is not in its K_n, the intersec-

tion of all the K_n must be zero. By Corollary 3.2, N is isomorphic to a subdirect sum of the nearrings N/K_n. Since each N/K_n has been shown to be subdirectly irreducible, the proof is complete.

The next theorem relates the radical of a nearring N to the subdirect sum structure of N, and shows that the primitive nearrings are "universal components" for the class of semisimple nearrings.

Theorem 3.5: A nonzero nearring is semisimple if and only if it is isomorphic to a subdirect sum of primitive nearrings.

Proof: If N is semisimple, the intersection of all of its primitive ideals is zero, so N is isomorphic to a subdirect sum of the nearrings N/P where P ranges over the set of primitive ideals of N. Each N/P is primitive by definition.

Conversely, if N is isomorphic to a subdirect sum of primitive nearrings N_i, let h be the isomorphism, let h_i be the natural homomorphism of Nh onto N_i, and let K_i be the kernel of the composite map hh_i. Then, $N_i = (Nh)h_i = N(hh_i)$, so N_i is isomorphic to N/K_i. It is easily verified that primitivity is preserved under isomorphism. Thus each K_i is primitive, so the radical J of N is contained in each K_i. But, by Corollary 3.2, the intersection of all the K_i is zero. Hence $J = (0)$, i.e., N is semisimple.

Logically, the next step is to establish a "good" representation theorem for primitive nearrings. For example, in ring theory each right primitive ring is isomorphic to a dense ring of linear transformations on a right vector space over a division ring. This representation problem has not been solved so satisfactorily for general nearrings.

For a restricted class of nearrings, the distributively generated nearrings satisfying the minimum condition, Laxton [11] has considered the representation problem for primitive nearrings. For the general problem, Theorem 4.8 shows that each primitive nearring N is isomorphic to a subnearring of the full transformation nearring of a difference group of $(N,+)$. It is hoped that the results of Chapters IV and V will be useful tools in a later, more successful, attack on this problem.

CHAPTER IV

FURTHER PROPERTIES OF NEARRINGS AND THE RADICAL

In this chapter a variety of properties of nearrings, especially primitive nearrings, and of the Jacobson radical will be established. Some of these results will be of use in Chapter V while others are of independent interest. Among the latter is Theorem 4.25 which shows that in a general nearring N the radical is hereditary in the sense that each invariant N-module (considered as a nearring) has as its radical the intersection of the module with the radical of N. A similar hereditary property holds for many, though not for all, of the radicals studied in rings.

The first concept to be considered will be convenient for use in the statement of some theorems and also helps to describe the structure of the kernel of an N-homomorphism. An <u>ideal</u> of an N-group G is a subset H of G such that

(1) $(H,+)$ is a normal subgroup of $(G,+)$, and

(2) $(g + h)n - gn$ is in H for each g in G, h in H, and n in N.

Thus the ideals of G mimic in G the properties of the right ideals of N. Notice, however, that an ideal of G may not

be an N-subgroup of G; if N is a nearring that is not special, the set {0} is an ideal of the N-group N, but {0} is not an N-subgroup of N.

Theorem 4.1: All ideals of an N-group G are N-groups, and hence N-subgroups of G, if and only if $0_G N = \{0_G\}$.

Proof: If $0_G N = \{0_G\}$, the conclusion is an obvious consequence of condition (2) in the definition of an ideal of an N-group. If all ideals of G are N-groups, then, in particular, $\{0_G\}$ is an N-group. Hence $0_G N \subseteq \{0_G\}$, so $0_G N = \{0_G\}$.

It is an immediate consequence of this theorem and Theorem 2.1 that every ideal of every N-group is itself an N-group if and only if N is special.

Beidleman [3] cites the dissertations of Betsch and R. J. Roth (at Tübingen and Duke, respectively) as the source of following characterization of the ideals of an N-group.

Theorem 4.2: H is an ideal of the N-group G if and only if H is the kernel of an N-homomorphism of G into some N-group G'.

Proof: If f is an N-homomorphism of G into G' with kernel H, then (H,+) is a normal subgroup of (G,+), because f is a group homomorphism. Consider the arbitrary elements g in G, h in H, and n in N, and let $x = (g + h)n - gn$. Then

$$xf = ((g + h)n - gn)f = (gf + hf)n - (gf)n = 0.$$

Thus x is in H, and H is an ideal of G.

If H is an ideal of the N-group G, let G' = (G,+) - (H,+) and let f be the natural group homomorphism of G onto G'. G' is made an N-group by the definition $(g + H)n = (gn + H)$ for each g in G and n in N. The only property needed that is not obvious is that the multiplication in G' by elements of N is well-defined. But if $(g_1 + H) = (g_2 + H)$, then $(-g_2 + g_1)$ is in H. Thus $(g_1n - g_2n)$, which is $(g_2 + (-g_2 + g_1))n - g_2n$, is in H for each n in N. Hence $(g_1n + H) = (g_2n + H)$, so $(g_1 + H)n = (g_2 + H)n$. Finally, for each g in G and n in N the computation $(gn)f = (gn + H) = (g + H)n = (gf)n$ shows that f is an N-homomorphism.

A concept and notation that will be convenient here, as in ring theory, is that of the Noetherian quotient of subsets of an N-group. Specifically, let S and T be subsets of an N-group G. The Noetherian quotient of T by S is defined by $(T:S) = \{n \in N \mid Sn \subseteq T\}$. In many instances these quotients are ideals or right ideals of the nearring N.

Theorem 4.3: Let H be an ideal of the N-group G and let S be any subset of G. Then

(1) (H:S) is a right ideal of N, and

(2) if $SN \subseteq S$ then (H:S) is an ideal of N.

Proof: Clearly, for each n_1 and n_2 in (H:S) and each s in S, $s(n_1 - n_2) = sn_1 - sn_2$ is in H. Thus (H:S) is a subgroup of (N,+). Also, for each m in N, each n in (H:S), and each s in S, $s(m + n - m) = sm + sn - sm$ is in H, because

$(H,+)$ is normal in $(G,+)$. Thus $(H:S)$ is normal in $(N,+)$. Finally, for each m_1 and m_2 in N, each n in $(H:S)$, and each s in S,

$$s((m_1 + n)m_2 - m_1m_2) = (sm_1 + sn)m_2 - (sm_1)m_2$$

is in H, because H is an ideal of G. Thus (1) has been established.

If $SN \subseteq S$, then $S(N(H:S)) = (SN)(H:S) \subseteq S(H:S) \subseteq H$. Thus $N(H:S) \subseteq (H:S)$, and the right ideal $(H:S)$ of N is an ideal of N.

Corollary 4.4: Let K be any right ideal of N, let G be any N-group, and let 0 be the identity element of G.

(1) $(K:S)$ is a right ideal of N for each subset S of N.

(2) $(K:N)$ is the largest ideal of N contained in K if K is modular.

(3) $(0:S)$ is a right ideal of N for each subset S of G.

(4) $(0:G) = A_G$

(5) $(0:g) = A_g$ for each g in G.

Proof: Results (1) and (3) are immediate consequences of the theorem. Results (4) and (5) are obvious restatements of definitions. For (2), assume K is modular and let e be the left identity modulo K. By definition of $(K:N)$, the product en is in K for each n in $(K:N)$. But $n - en$ is also in K for each n in $(K:N)$, and hence $(K:N) \subseteq K$. Let L be any ideal of N such that $(K:N) \subseteq L \subseteq K$. Then for each k in L, $Nk \subseteq L \subseteq K$, i.e., k is in $(K:N)$. Thus $(K:N) = L$.

The next three theorems, all of which are direct analogs of results in ring theory (see McCoy [14]), relate Noetherian quotients of ideals to primitive nearrings and lead up to Theorem 4.8, a representation theorem for primitive nearrings. The first of these theorems is restricted to special nearrings; the others are not.

Theorem 4.5: If K is an m-minimal right ideal of the special nearring N and if $K^2 \neq \{0\}$, then N/(0:K) is a primitive nearring.

Proof: Denote N/(0:K) by $\overline{N}$. K is nonzero, for otherwise it would not be m-minimal. K is an N-module because N is special. Hence K, being m-minimal, is a minimal N-group. For each n in N let $\overline{n}$ be the element n + (0:K) in $\overline{N}$, and define a multiplication by $k\overline{n} = kn$ for each k in K and $\overline{n}$ in $\overline{N}$. It is easily verified that, with this multiplication, K is a minimal $\overline{N}$-group. Also, $K\overline{N} = KN$ is nonzero because K^2 is nonzero. Hence K is an essentially minimal $\overline{N}$-group. Finally, the annihilator ideal of K in $\overline{N}$ is $(\overline{0})$, for if $\{0\} = K\overline{n} = Kn$, then n is in (0:K), i.e., $\overline{n} = \overline{0}$. Thus the nearring N/(0:K), and hence also the ideal (0:K) of N, is primitive.

Theorem 4.6: If K is an m-maximal right ideal of the nearring N, and if $N^2 \not\subseteq K$, then N/(K:N) is primitive.

Proof: Denote N/(K:N) by $\overline{N}$. K is not all of N, for otherwise it would not be m-maximal. Let $\underline{N}$ be the nonzero difference group (N,+) - (K,+). For each n in N let $\underline{n}$ be

the element n + K in $\underline{N}$, let $\overline{n}$ be the element n + (K:N) in $\overline{N}$, and define $\underline{m}\overline{n} = \underline{mn}$ for all m and n in N. It is easily verified that, with this multiplication, $\underline{N}$ is a minimal $\overline{N}$-group. Also, $\underline{N}\overline{N} = \underline{NN}$ is nonzero because N^2 is not in K. Hence $\underline{N}$ is an essentially minimal $\overline{N}$-group. Finally, the annihilator ideal of $\underline{N}$ in $\overline{N}$ is $(\overline{0})$, for if $\{\underline{0}\} = \underline{N}\overline{n} = \underline{Nn}$, then n is in (K:N), i.e., $\overline{n} = \overline{0}$. Thus the nearring N/(K:N), and hence also the ideal (K:N) of N, is primitive.

These last two proofs could be shortened, conceptually, by an application of Lemma 2.5, which says that the annihilator ideal of an essentially minimal $\overline{N}$-group is primitive. With this, the proof of Theorem 4.5 is complete once K has been shown to be an essentially minimal $\overline{N}$-group. In the proof of Theorem 4.6, however, it still must be argued that $(\underline{0}:\underline{N})$ = (K:N), and this argument prevents any effective shortening of the proof. The proofs given also exhibit the same duality that is obvious in the statements of these two theorems.

Theorem 4.7: If K is a modular m-maximal right ideal of the nearring N, then N/(K:N) is primitive. A nearring N is primitive if and only if it contains a modular m-maximal right ideal K such that (K:N) is the zero ideal.

Proof: There is some n in N that is not in K since K is m-maximal. Because K is modular, (n - en) is in K, where e is the left identity modulo K. Hence en is not in K, for

otherwise n must be in K. Thus $N^2 \not\subseteq K$, and the first statement follows from the preceding theorem.

If (K:N) = (0), then N is isomorphic to N/(K:N), so N is primitive by the first statement of this theorem.

If N is primitive there exists an essentially minimal N-group G with $A_G = (0)$. By Theorem 2.7, there is a g in G such that gN = G and A_g is a modular m-maximal right ideal of N. Let $K = A_g$. If n is in (K:N), then $Nn \subseteq K$, so $gNn = \{0\}$. But gN = G, so $Gn = \{0\}$. Thus n is in $A_G = (0)$, so (K:N) = (0), and the proof is complete.

Theorem 4.8: Each primitive nearring N is isomorphic to a nearring of transformations on a difference group of (N,+).

Proof: If N is primitive, there is, by Theorem 4.7, a modular m-maximal right ideal K of N such that (K:N) = (0). Let G be the group (N,+) - (K,+), and let T be the nearring of all transformations of G into itself. Consider the map f of N into T defined for each x in N by $(n + K)(xf) = nx + K$. By the definitions of addition and multiplication in T, f is seen to be a nearring homomorphism. Also, the kernel of f is {0}, for if xf = 0 in T, then (nx + K) = K for each n in N, and hence x is in (K:N) = (0). Thus N is isomorphic to a subnearring of T.

An essentially minimal N-group G such that $A_G = (0)$ will be called a primitive N-group. By definition, N has a

primitive N-group if and only if N is a primitive nearring.

Nearfields are primitive. This will be established (Theorem 5.4) in the next chapter, as will the fact (Theorem 5.2) that a nearfield has only the two trivial ideals. Of more direct interest here is the result that for a nearfield N the primitive N-groups and essentially minimal N-groups coincide. A somewhat more general statement holds.

Theorem 4.9: If N is a primitive nearring that has only the two trivial ideals, (0) and N, then an N-group G is primitive if and only if it is essentially minimal.

Proof: Any primitive N-group is essentially minimal, by definition. Conversely, if G is essentially minimal, then $GN \neq \{0\}$. Thus $A_G \neq N$, so A_G must be (0), the only other ideal of N.

Corollary 4.10: If N is a nearfield, then an N-group is primitive if and only if it is essentially minimal.

Each nearfield, as well as each of the nearrings mentioned in Chapter I, has a two-sided identity. From a purely abstract viewpoint, however, it is clear that the assumption that a nearring has an identity, even a one-sided identity, is a major restriction. The existence of an identity has many consequences concerning the structure of a nearring. For example, if a nearring has a left identity then every right ideal is modular. For a second example, if N is an arbitrary nearring it is not at all obvious (it is, in

fact, unknown) whether or not $gN = G$ for each nonzero g in an essentially minimal N-group G. However, if N has a right identity, this property is characteristic of essentially minimal N-groups.

Theorem 4.11: If N is a nearring with right identity e, then a nonzero N-group G is essentially minimal if and only if $gN = G$ for each nonzero g in G.

Proof: If $gN = G \neq \{0\}$ for each nonzero g in G, and if H is any nonzero N-subgroup of G, then $G = HN \subseteq H \subseteq G$. Thus $H = G$, and G is essentially minimal.

Conversely, if G is an essentially minimal N-group, then by Theorem 2.7 there is a g' in G such that $g'N = G$. Thus for each g in G there is an n_g in N such that $g = g'n_g$. Hence for each nonzero g in G, $g = g'n_g = g'(n_g e) = (g'n_g)e = ge$ is in gN. Thus $gN \neq \{0\}$. But gN is an N-subgroup of G and G is minimal, so $gN = G$.

If attention is restricted to primitive nearrings, the assumption that a right identity exists yields an even stronger conclusion. In fact, a right identity in a primitive nearring is a two-sided identity. A portion of the proof will be stated as a lemma which is of some independent interest. Following Jacobson [9], an N-group G will be called unital if N has a right identity e and $ge = g$ for each g in G.

Lemma 4.12: If N has a right identity e, then each essentially minimal N-group G is unital.

Proof: As in the proof of Theorem 4.11, because G is essentially minimal there is a g' in G such that for each g in G there is an n_g in N for which $g = g'n_g$. Hence for each g in G, $g = g'n_g = g'(n_g e) = (g'n_g)e = ge$.

Theorem 4.13: A right identity e in a primitive near-ring N is a two-sided identity.

Proof: Let G be a primitive N-group. By the lemma G is unital. Hence, $0 = gn - gen = g(n - en)$ for each g in G and n in N. Thus $(n - en)$ is in A_G. But $A_G = (0)$, so $n = en$ for each n in N.

Corollary 4.14: In a nearring N with right identity e, each primitive ideal is modular.

Proof: Let K be a primitive ideal of N. Then N/K is primitive with right identity $(e + K)$. By the theorem $(e + K)$ is also a left identity in N/K, so e is a left identity modulo K.

Recall that an N-module M is an N-subgroup of (N,+) and that M is invariant if $NM \subseteq M$. Since M need not be a normal subgroup of (N,+), the N-modules are distinct from the right ideals of N. Indeed, each N-module is a subnear-ring of N, though a right ideal of N need not be. If and only if N is special do the right ideals of N form a subset of the N-modules. If N is a ring, or any special nearring with commutative addition, the two concepts coincide. This

last statement hints of the importance of modules in the theory of nearrings. Some of the properties of an ideal in a ring come from its structure as an ideal in a nearring, others come from its structure as a nearring module.

The next few pages will lead up to Theorem 4.25, mentioned at the start of this chapter, which says that with respect to invariant modules the radical of a general nearring is hereditary. This will illustrate the comments of the preceding paragraph, for it is a natural generalization of a result in the theory of rings concerning the hereditary behavior with respect to ideals of the Jacobson radical of a ring. As a first step it will be shown that primitivity is hereditary in this generalized sense.

Theorem 4.15: A nonzero invariant N-module M of a primitive nearring N is itself a primitive nearring.

Proof: It is immediate that an N-module is a subnearring of N. Let G be a primitive N-group. It is obvious that G can be regarded as an M-group and that the annihilator ideal of G in M is (0). Only the minimality of G as an M-group needs to be established. To do this, let H be a nonzero M-subgroup of G. There are two cases to be considered.

If $HM \neq \{0\}$, then $hM \neq \{0\}$ for some h in H. But $(hM)N = h(MN) \subseteq hM$, because M is an N-module. Thus hM is a nonzero N-subgroup of G, so $hM = G$. Hence $G = HM \subseteq H \subseteq G$, so $H = G$.

If $HM = \{0\}$, it may be assumed that $HN \neq \{0\}$, for otherwise H is a nonzero N-subgroup of G, whence $H = G$. Now, $HN \neq \{0\}$ implies $hN \neq \{0\}$ for some h in H. Thus, since hN is an N-subgroup of G, $hN = G$ and $HN = G$. But, because M is invariant, $GM = (HN)M = H(NM) \subseteq HM = \{0\}$. This implies $M \subseteq A_G = (0)$, which contradicts the assumption that $M \neq (0)$. In each case then, $H = G$.

Thus the only possible M-subgroups of G are $\{0\}$ and G, so G is indeed a minimal M-group, and the proof is complete.

An immediate corollary of this theorem is the well-known result that each nonzero ideal in a primitive ring is itself a primitive ring. Somewhat more generally, if K is a nonzero ideal of the primitive nearring N, then $(kn - 0n)$ is in K for each k in K and n in N. It follows that if $0N \subseteq K$, then $KN \subseteq K$. Also, $NK \subseteq K$ because K is an ideal, so K may act as the invariant N-module M in Theorem 4.15. Two corollaries to the theorem are then evident.

Corollary 4.16: A nonzero ideal K of a primitive nearring N is itself a primitive nearring if $ON \subseteq K$.

Corollary 4.17: A nonzero ideal K of a primitive special nearring N is itself a primitive special nearring.

Another result that follows from Theorem 4.15 concerns primitive ideals and N-modules.

Corollary 4.18: A primitive ideal P of a nearring N is also a primitive ideal of any invariant N-module M (considered as a nearring) which properly contains P.

Proof: A straightforward check of the required properties shows that $\overline{M} = (M/P,+)$ is a nonzero invariant (N/P)-module. Since N/P is primitive, the conclusion follows from Theorem 4.15 and the definition of a primitive ideal.

In particular, a primitive ideal P of a special nearring N is also a primitive ideal of any ideal Q of N that properly contains P.

Notice that the radical has been defined only for nearrings. Whenever the radical of an ideal K or of an N-module M is mentioned, it is the radical of the nearring K or the nearring M that is meant. With the aid of a pair of lemmata, one half of the hereditary property of the radical is easily obtained from Theorem 4.15. The first lemma is a special case of a theorem due to R. J. Roth, cited by Beidleman in [3]; the second lemma is one form of the "Second Isomorphism Theorem" for nearrings.

Lemma 4.19: If K is a right ideal of the nearring N and M is an N-module, then $K + M = \{k + m | k \in K, m \in M\}$ is an N-module.

Proof: Certainly, $K + M = M + K$ is a subgroup of $(N,+)$, since M is a subgroup and K is a normal subgroup of $(N,+)$. For each m in M, each k in K, and each n in N, $(m + k)n - mn$ is in K and mn is in M, so $(m + k)n$ is in $K + M$. Thus $K + M$ is an N-module.

Lemma 4.20: If K is an ideal of the nearring N and M is an N-module, then $(M + K)/K$ is isomorphic to $M/(M \cap K)$.

Proof: By Lemma 4.19, $M + K$ is an N-module, hence a subnearring. Obviously, K is an ideal of $M + K$, so $(M + K)/K$ is a nearring. Clearly, from group theory, $M \cap K$ is a normal subgroup of $(M,+)$. Also $MN \subseteq M$ and $NK \subseteq K$ imply $M(M \cap K) \subseteq M \cap K$. Finally, because K is a right ideal and M is a subnearring, $(m_1 + x)m_2 - m_1m_2$ is in $M \cap K$ for each m_1 and m_2 in M and x in $M \cap K$. Thus $M \cap K$ is an ideal of M, so $M/(M \cap K)$ is a nearring. It is easily checked that the map f defined by $(m + k + K)f = m + (M \cap K)$ is the required isomorphism from $(M + K)/K$ to $M/(M \cap K)$.

Theorem 4.21: If N is a nearring with radical J, if M is an invariant N-module, and if I is the radical of M, then $I \subseteq M \cap J$. In particular, if N is semisimple, so also is M.

Proof: If $M \subseteq J$ the conclusion is obvious. If $M \not\subseteq J$, let P be any primitive ideal of N such that $M \not\subseteq P$. Such a P must exist, by Theorem 2.6. Now, $M + P$ is an N-module, by Lemma 4.19, and it is clear that $M + P$ properly contains P and that $N(M + P) \subseteq M + P$. Hence, by Corollary 4.18, $(M + P)/P$ is primitive, and so, by Lemma 4.20, $M/(M \cap P)$ is primitive.

Thus $M \cap P$ is a primitive ideal of M for each primitive ideal P of N such that $M \not\subseteq P$. By Theorem 2.6 applied to M then, the radical I of M is contained in $\cap\{M \cap P \mid P \text{ is a primitive ideal of } N\} = M \cap J$.

The completion of the proof of the hereditary property of the radical, i.e., the proof that $M \cap J \subseteq I$ in the notation of Theorem 4.21, makes use of modular m-maximal right ideals instead of the primitive ideals used in the preceding proof. The key step is given in

Lemma 4.22: For each N-module M and each modular m-maximal right ideal K of the nearring M, there is a modular m-maximal right ideal L of N such that $L \cap M = K$.

Proof: By Theorems 2.7 and 2.8, $G = (M,+) - (K,+)$ is an essentially minimal M-group. As in Theorem 2.8, the multiplication of G by M is given by $\overline{m}_1 m_2 = \overline{m_1 m_2}$ where $\overline{x}$ denotes the element $(x + K)$ of G. Let e be a left identity modulo K in M. Then $(m - em)$ is in K for each m in M. It follows that $\overline{e}M = G$, because, for each $\overline{m}$ in G, $\overline{m} = \overline{em} = \overline{e}m$ is in $\overline{e}M$. The annihilator right ideal of $\overline{e}$ in M is K, for $\overline{e}m = \overline{0}$ if and only if em is in K. But $m - em$ is in K, and so em is in K if and only if m is in K.

With the definition $\overline{m}n = \overline{mn}$ for each $\overline{m}$ in G and n in N, G may be considered as an N-group. G is minimal as an N-group, because any N-subgroup of G would be an M-subgroup of the minimal M-group. Because $\{\overline{0}\} \neq GM \subseteq GN$, G is an essentially minimal N-group. Also, $G = \overline{e}M \subseteq \overline{e}N \subseteq G$, so $\overline{e}N = G$. Let L be the annihilator right ideal of $\overline{e}$ in N. For each m in $L \cap M$, $\overline{e}m = \overline{0}$, so em is in K. Since $(m - em)$ is in K also, m is in K. Conversely, for each m in K, $\overline{e}m = \overline{0}$, so m is in L. Thus $L \cap M = K$.

Corollary 4.23: If an N-module M is considered as a nearring, each essentially minimal M-group G can be M-isomorphically embedded in an essentially minimal N-group.

Proof: By Theorems 2.7 and 2.8, there is a g in G such that G = gM is M-isomorphic to (M,+) - (K,+), where K is the annihilator right ideal of g in M and K is modular and m-maximal. By the lemma, there is a modular m-maximal right ideal L of N such that $L \cap M = K$. Again, by Theorems 2.7 and 2.8, G' = (N,+) - (L,+) is an essentially minimal N-group. It is easily verified that the map f defined by $(m + K)f = (m + L)$ is an M-isomorphism of (M,+) - (K,+) into G'.

The second half of the hereditary property can now be established under hypotheses slightly less restrictive than those required for the first half, Theorem 4.21; it is not required here that the N-module M be invariant.

Theorem 4.24: If N is a nearring with radical J and M is an N-module with radical I, then $M \cap J \subseteq I$.

Proof: If I = M the conclusion is obvious. Assume then $I \neq M$. By Theorem 2.9, when the radical is a proper ideal it is the intersection of all the modular m-maximal right ideals of the nearring. For each modular m-maximal right ideal K of M let K' be a modular m-maximal right ideal of N (given by Lemma 4.22) such that $M \cap K' = K$. Let X be the set of all such right ideals K of M, let Y be the set of all the corresponding right ideals K' of N, and let Z be the

set of all modular m-maximal right ideals of N. Then $M \cap J = M \cap \{\cap L | L \varepsilon Z\} = \cap \{M \cap L | L \varepsilon Z\}$, and thus $M \cap J \subseteq \cap \{M \cap K' | K' \varepsilon Y\} = \cap \{K | K \varepsilon X\} = I$. Notice that the hypothesis $I \neq M$ implies that Z is not empty, i.e., that $J \neq N$. For if Z is empty, it follows from Lemma 4.22 that there is no modular m-maximal right ideal of M, and hence $I = M$.

Theorem 4.25: If N is a nearring with radical J, if M is an invariant N-module, and if I is the radical of M, then $I = M \cap J$.

Proof: Theorem 4.21 and Theorem 4.24.

Just as Theorem 4.15 produced Corollaries 4.16 and 4.17, each of the theorems of these last few pages can be specialized by taking the N-module M to be an ideal of N. For example, Theorem 4.25 yields

Corollary 4.26: If N is a nearring with radical J, if K is an ideal of N such that $0N \subseteq K$, and if I is the radical of K, then $I = K \cap J$.

Corollary 4.27: If N is a special nearring with radical J and K is an ideal of N with radical I, then $I = K \cap J$.

From this last result there follows immediately

Corollary 4.28: The radical J of a special nearring N is itself a radical nearring, i.e., the radical of J is J.

It is now clear how the hereditary property of the radical is affected as the ascent is made from rings to more

general nearrings. It is with respect to invariant nearring modules that the radical is hereditary. This is obscured in rings by the fact that the modules and ideals coincide. Even in special nearrings the hereditary property is obscured to some extent because each ideal is a module. It is in general nearrings, where module properties and ideal properties are distinct, that the true situation is seen most plainly.

The relationship of the radical of N with the nil and nilpotent N-modules will now be considered. Recall that Betsch showed (Theorem 2.10) that a special nearring N with minimum condition is semisimple if and only if $\{0\}$ is the only nilpotent N-module. One half of this theorem holds more generally. The radical contains each module that is "nilpotent modulo the radical". This is stated more precisely as

Theorem 4.29: If N is a nearring with radical J, and if M is an N-module such that $M^k \subseteq J$ for some positive integer k, then $M \subseteq J$.

Proof: If $M \not\subseteq J$ there must be some minimal N-group G such that $GM \neq \{0\}$, and hence some g in G such that $gM \neq \{0\}$. But gM is an N-subgroup of the minimal N-group G, so $gM = G$. Thus $GM = G$, and it follows that $\{0\} \neq G = GM = GM^2 = \cdots = GM^k$. But $M^k \subseteq J$, and so $GM = GM^k = \{0\}$, which is a contradiction. Thus $M \subseteq J$.

Corollary 4.30: The radical J of N contains every nilpotent N-module M.

Proof: There is some positive integer k such that $M^k = \{0\}$. Obviously, $\{0\} \subseteq J$.

Corollary 4.31: If N is semisimple then $\{0\}$ is the only possible nilpotent N-module.

Proof: If $\{0\}$ is an N-module it is certainly nilpotent. (It was remarked earlier that if N is not special $\{0\}$ is not an N-module.)

A proof similar to that of Theorem 4.29 holds for nil N-modules in special nearrings.

Theorem 4.32: If N is special each nil N-module M is contained in the radical J of N.

Proof: If $M \not\subseteq J$ there must be some minimal N-group G such that $GM \neq \{0\}$, and hence some g in G such that $gM \neq \{0\}$. But, being a nonzero N-subgroup of the minimal N-group G, $gM = G$. Thus there is some m in M such that $gm = g$, so $g = gm = gm^2 = \cdots$. But m is in M, so m is nilpotent, say $m^k = 0_N$. Then $g = gm = \cdots = gm^k = g0_N = 0_G$, so $G = gM = 0_G M$. By Theorem 2.1, $0_G M = \{0_G\}$, because N is special. But G is minimal, so $G \neq \{0_G\}$. To avoid the contradiction, M must be contained in J.

The last two theorems show that certain N-modules are known to be contained in the radical. The next theorem and its corollary identify certain right ideals that are contained in the radical of a special nearring.

Theorem 4.33: If N is a nearring with radical J and M is an N-module such that $M \not\subseteq J$, then either M is essentially minimal or M contains a proper nonzero ideal of the N-group M.

Proof: Since $M \not\subseteq J$ there is an essentially minimal N-group G such that $GM \neq \{0\}$. Hence, by a now familiar argument, there is a g in G such that $gM = G$. By Theorem 2.8, G is N-isomorphic to the difference N-group $\overline{M} = (M,+) - (A_g \cap M,+)$. Now, the natural map f from M to $\overline{M}$, defined by $(m)f = \overline{m}$, is an onto homomorphism and is easily seen to be an N-homomorphism. Thus either $A_g \cap M = \{0\}$ and M is isomorphic to G, or $A_g \cap M$, being the nonzero kernel of an N-homomorphism, is a nonzero ideal of the N-group M. In the latter case, $A_g \cap M \neq M$ because $\overline{M}$ is isomorphic to G which is nonzero.

Corollary 4.34: The radical of a special nearring N contains each minimal right ideal K of N that is not m-minimal.

Proof: Let K be the N-module M in the theorem. Since K is a right ideal, so also is $A_g \cap K$. Because K is minimal as a right ideal, it cannot properly contain a nonzero right ideal of N. The theorem then allows only two possible conclusions: either K is essentially minimal as an N-group, in which case K is clearly m-minimal; or K is contained in the radical of N.

Just as minimal right ideals can be related to the radical (at least in special nearrings), so also can maximal right ideals.

Theorem 4.35: Each nilpotent right ideal K of a nearring N is contained in each modular maximal right ideal H of N.

Proof: Assume $K^n = (0)$. If $K \not\subseteq H$, then $K + H = N$ because the sum of right ideals is a right ideal and H is maximal. Let e be a left identity modulo H and let $e = k + h$, where k is in K and h is in H.

By assumption, $K^n \subseteq H$. The proof proceeds by induction on the exponent n. Assume $K^m \subseteq H$ for some integer $m > 1$, and let k_{m-1} be in K^{m-1}. Then $ek_{m-1} = ((k + h)k_{m-1} - kk_{m-1}) + kk_{m-1}$ is in $H + K^m = H$. Thus ek_{m-1} is in H. But $(k_{m-1} - ek_{m-1})$ is also in H for each k_{m-1} in K^{m-1}, so $K^{m-1} \subseteq H$. By induction, $K \subseteq H$, contrary to assumption. To avoid this contradiction, $K \subseteq H$.

Corollary 4.36: If the radical J of N is nilpotent, J is contained in each modular maximal right ideal of N.

Proof: J is a right ideal of N.

Corollary 4.37: If the radical J of a special nearring N is nilpotent, then J is the intersection of all the modular maximal right ideals of N.

Proof: Let I be the intersection in question. By Corollary 4.36, $J \subseteq I$. Because N is special, each right

ideal is a module, so each module-maximal right ideal is surely maximal as a right ideal. Then I, the intersection of all the modular maximal right ideals of N, is contained in the intersection of those that are only m-maximal, and that intersection is J. Thus $I \subseteq J$, so $I = J$.

CHAPTER V

NEARFIELDS AND SUBDIRECT SUMS

A nearfield is a nearring in which the nonzero elements form a group under multiplication. Since a group is a nonempty set, a nearfield contains at least two distinct elements, the additive and multiplicative identities. Because multiplicative inverses exist for nonzero elements, a nearfield has no nonzero divisors of zero.

In 1936 Zassenhaus [17] showed that the additive group of any finite nearfield must be commutative. In 1940 B. H. Neumann [15] extended this result to all nearfields. Thus a (left) nearfield satisfies all the axioms of a division ring except, possibly, the right distributive law. It is not surprising then that a nearfield with some restriction on its multiplicative group frequently turns out to be a field or division ring. The next few theorems establish some useful properties of nearfields. The symbol e will be used for the multiplicative identity.

Theorem 5.1: A nearfield is a special nearring.

Proof: If N is a nearfield and there is some element n in N such that $0n \neq 0$, then 0n must have a multiplicative

inverse m. For each x in N it follows that x = xe = x(m(0n)) = (xm0)n = 0n. Thus 0n is the only element of N, which contradicts the fact that a nearfield must have more than one element.

Theorem 5.2: A nearfield N has exactly two ideals, (0) and N.

Proof: If K is an ideal of N, then $NK \subseteq K$. Assume that $K \neq (0)$, and let k be a nonzero element of K. Now k has a multiplicative inverse h, so hk = e is in K. Thus ne = n is in K for each n in N, and hence K = N.

Corollary 5.3: A nearfield is subdirectly irreducible.

Proof: This is an immediate consequence of Theorem 5.2 and Corollary 3.3.

Theorem 5.4: A nearfield N is primitive.

Proof: M = (N,+) is an N-group. If M' is any nonzero N-subgroup of M, then any nonzero element m in M' has a multiplicative inverse n in N. Thus mn = e is in M'N which is contained in M'. Hence en = n is in M' for each n in N, so M' = N = M, i.e., M is minimal. Since e is in M, A_M = (0). Thus M is an essentially minimal N-group whose annihilator ideal is zero, i.e., N is primitive.

An immediate corollary of this proof is that a nearfield has only two N-modules, {0} and (N,+). A more general result will be proved in Corollary 5.16.

Theorem 5.5: If N/K is a nearfield, then K is a maximal ideal of the nearring N.

Proof: Because a nearfield has more than one element, K must be a proper ideal of N. Let m be any element of N that is not in K and let n be any element of N. Then $\overline{m} = (m + K) \neq K = \overline{0}$, and since N/K is a nearfield there is an $\overline{x} = \overline{n}(\overline{m})^{-1}$ in N/K such that $\overline{xm} = \overline{x}\,\overline{m} = \overline{n}$. Hence there is a k in K such that xm + k = n. But n is arbitrary in N, so it has been shown that the ideal generated by K and any element of N not in K is all of N, i.e., K is maximal in N.

Certain properties of nearfields will carry over to any subdirect sum of nearfields. For example, any subdirect sum of nearfields must have commutative addition and must be a special nearring. Only slightly less obvious than this is

Theorem 5.6: If N is isomorphic to a subdirect sum of the nearfields N_i, then N is semisimple and the intersection of all the maximal ideals of N is the zero ideal.

Proof: The first claim is an immediate result of Theorems 5.4 and 3.5. By the definition of subdirect sum there exist homomorphisms h_i of N onto N_i. Let K_i be the kernel of h_i. Then N/K_i is isomorphic to the nearfield N_i, so by Theorem 5.5 each K_i is a maximal ideal of N. It follows from Theorem 3.1 that for each nonzero element n in N there is some K_i such that n is not in K_i. Hence the intersection of all the K_i is the zero ideal.

Lemma 5.7: If K is a maximal ideal in a nearring N, then the zero ideal is maximal in N/K.

Proof: A straightforward check of the defining properties of an ideal shows that, if N/K had a nonzero proper ideal $\overline{I}$, then $I = \{n \in N \mid \overline{n} = (n + K) \in \overline{I}\}$ would be a proper ideal of N that properly contains K. This is impossible, so the zero ideal is maximal in N/K.

Theorem 5.8: Let N be a nearring in which multiplication is commutative. The difference nearring N/K is a field (not just a nearfield) if and only if K is a modular maximal right ideal of N.

Proof: Assume K is a modular maximal right ideal of N. Because N has commutative multiplication, $0n = n0 = 0$ for each n in N, so N is special and $nk = kn - 0n = (0 + k)n - 0n$ is in K for each n in N. Thus K is an ideal of N. Also, the multiplication in N/K inherits commutativity from that in N. Let e be the left identity modulo K. Then $\overline{e} = (e + K)$ is an identity in N/K. Thus N/K is a nearring with identity in which multiplication is commutative. Berman and Silverman show in [4] that under these conditions N/K is a commutative ring with identity. Such a ring is a field if and only if the zero ideal is maximal. By the lemma then, N/K is a field.

Conversely, if N/K is a field it is a nearfield. By Theorem 5.5, K is a maximal ideal of N. As before, each

right ideal of N is an ideal, because multiplication is commutative. Hence K, being maximal as an ideal of N, must also be maximal as a right ideal. Let $\overline{e} = (e + K)$ be the identity of N/K. Then $\overline{n} = \overline{en}$ for each n in N, so (n - en) is in K for each n in N. Thus K is modular.

Theorem 5.9: A nearring N has commutative multiplication and is primitive if and only if it is a field.

Proof: If N is a field it has commutative multiplication. Also, a field is a nearfield and therefore primitive.

Conversely, if N is a primitive nearring with commutative multiplication, there is, by Theorem 4.7, a modular m-maximal right ideal K of N such that (K:N) = (0). By commutativity, N is special and K is a modular ideal. Hence $NK \subseteq K$, so $K \subseteq (K:N) = (0)$. Thus (0) is a modular m-maximal ideal. Because multiplication is commutative, each right ideal of N is an N-module. Hence (0), being an m-maximal ideal, must also be maximal as a right ideal. It now follows from Theorem 5.8 that N is a field.

Corollary 5.10: A nonzero nearring N with commutative multiplication is semisimple if and only if it is isomorphic to a subdirect sum of fields.

Proof: This is a direct consequence of Theorems 3.5 and 5.9.

Corollary 5.11: A semisimple nearring with commutative multiplication is a ring.

Thus the semisimple nearrings with commutative multiplication have been completely determined. Such a nearring is either the zero ring or is isomorphic to a subdirect sum of fields.

If J is the radical of the nearring N, it is known (Theorem 2.3) that N/J is semisimple. It follows immediately from Corollary 5.11 that if multiplication is commutative in N/J then N/J is a commutative ring. This result can be stated in terms of elements in the radical J as

Corollary 5.12: In the nearring N with radical J, if mn - nm is in J for each m and n in N, then (m + n) - (n + m) is in J for each m and n in N.

Proof: The hypothesis is that N/J has commutative multiplication; the conclusion is that N/J has commutative addition. A nearring with commutative addition and multiplication is a commutative ring.

As an example of a nearring with commutative multiplication that is not semisimple, let N be any noncommutative group in additive notation. Define mn = 0 for all m and n in N. With this multiplication, N is a nearring with commutative multiplication that is not a ring. This example is a special nearring. Indeed, it is a distributively generated nearring. (A nearring is distributively generated if there is a subsemigroup S of right distributive elements of the multiplicative semigroup which generates the nearring additively. Each distributively generated nearring is a

special nearring.) Since every element annihilates all of N, this example is a radical nearring, that is, the radical is all of N.

Let J be the radical of a nearring N. Because the radical of N/J is the zero ideal, there follows immediately from Corollary 5.10

Corollary 5.13: A nearring N with commutative multiplication is either a radical nearring or it has a homomorphic image which is a subdirect sum of fields.

In order to relax the restriction of Theorem 5.8 to nearrings in which multiplication is commutative, the concept of modularity will now be extended. An ideal K of a nearring N will be called right modular if there exists an element e' in N such that (n - ne') is in K for each n in N, and such an element e' will be called a right identity modulo K. If K is both modular and right modular, K will be called bimodular.

In a nearring with identity element it is obvious that all ideals are bimodular. A less trivial example is given by the ring qZ/pqZ, where p and q are distinct primes. (Here the symbol kZ represents the ring of all integral multiples of k, and qZ/pqZ represents the ring of residue classes.) Since qZ/pqZ is isomorphic to the integers modulo p, it is a field. Thus qZ/pqZ has an identity element, although qZ itself does not. It follows that the ideal pqZ of the ring

qZ must be bimodular. Similarly, if N/K is a nearring with identity, then K is a bimodular ideal of N.

Theorem 5.14: A difference nearring N/K is a nearfield if and only if K is a bimodular m-maximal ideal of N.

Proof: If K is bimodular there exist e and e' in N such that (n - en) and (n - ne') are in K for each n in N. Hence $\overline{e} = (e + K)$ is a left identity and $\overline{e'} = (e' + K)$ is a right identity in N/K, so $\overline{e} = \overline{e}\,\overline{e'} = \overline{e'}$, and thus $\overline{e}$ is a two-sided identity in N/K.

Now K is a modular m-maximal right ideal of N, so, by Theorems 2.7 and 2.8, G = (N,+) - (K,+) is an essentially minimal N-group. By the definition $g\overline{n} = gn$ for each g in G and each $\overline{n} = (n + K)$ in N/K, G is made into an essentially minimal (N/K)-group. If g is any nonzero element of G, then g(N/K) is an (N/K)-subgroup of G, so g(N/K) = {0} or g(N/K) = G. But g(N/K) = {0} implies that $g\overline{e} = 0$, which cannot be since $\overline{e}$ is an identity in N/K and $g = (n + K)$ for some n in N. Thus g(N/K) = G, so there is an m in N such that $g(m + K) = (e + K) = \overline{e}$, i.e., each nonzero element of N/K has a right (multiplicative) inverse in N/K. Hence the nonzero elements of N/K form a group under multiplication, i.e., N/K is a nearfield.

Conversely, if N/K is a nearfield with identity (e + K), then e is clearly a right and left identity modulo K, so K is bimodular. If K is properly contained in an N-module L, then the image L' of L under the natural homomorphism of N

onto N/K is a nonzero (N/K)-module. By the remark following Theorem 5.4 it follows that L' = N/K, so L = N. Thus K is m-maximal and the proof is complete.

Corollary 5.15: A nearring N is a nearfield if and only if N has an identity and the zero ideal is m-maximal.

Proof: N has an identity if and only if the zero ideal is bimodular.

Corollary 5.16: A nonzero nearring N with identity is a nearfield if and only if {0} and (N,+) are the only N-modules.

Proof: It was observed just after Theorem 5.4 that in a nearfield N the only N-modules are {0} and (N,+). If N is a nonzero nearring with identity having only the two N-modules {0} and (N,+), then (0) is a bimodular m-maximal ideal of N.

Corollary 5.17: A difference nearring N/K is a nearfield if and only if K is an m-maximal primitive right modular ideal of N.

Proof: If N/K is a nearfield then K is bimodular and m-maximal by Theorem 5.14. Since a nearfield is primitive, K is also primitive.

Conversely, if K is primitive and right modular, then K is bimodular by Theorem 4.13. Thus if K is m-maximal, primitive, and right modular, it is m-maximal and bimodular. By Theorem 5.14 then, N/K is a nearfield.

Corollary 5.18: A nearring N with right identity e is a nearfield if and only if N is primitive and (N,+) is the only nonzero N-module.

Proof: If N is a nearfield, then N is nonzero and has an identity. By Corollary 5.16, (N,+) is the only nonzero N-module. By Theorem 5.4, N is primitive.

Conversely, if N is primitive and has right identity e, and if (N,+) is the only nonzero N-module, then (0) is right modular, primitive and m-maximal. By Corollary 5.17, N is a nearfield.

It is well-known (Barnes [1] p. 126) that, given a commutative ring R with an ideal M, R/M is a field if and only if M is a maximal ideal of R and x is in M whenever x^2 is in M. One generalization of this theorem for arbitrary nearrings substitutes a third condition for the commutativity of multiplication.

Theorem 5.19: A difference nearring N/K is a nearfield if and only if the following three conditions are satisfied.

(1) K is an m-maximal ideal of N.

(2) If x^2 is in K then x is in K.

(3) For each y in N but not in K and for each n in N, there is an m in N such that yn - my is in K.

Proof: If N/K is a nearfield, then K is a bimodular m-maximal ideal of K, by Theorem 5.14. Since a nearfield has no nonzero divisors of zero, $\overline{x}^2 = \overline{0}$ implies $\overline{x} = \overline{0}$, i.e.,

x^2 in K implies x is in K. Finally, if y is in N but not in K, then $\bar{y}$ has a multiplicative inverse $\bar{y}^{-1}$ in N/K. Given n in N, define $\bar{m} = \bar{y}\ \bar{n}\ \bar{y}^{-1}$. Then $\overline{my} = \overline{yn}$, so yn - my is in K.

Conversely, if (1), (2), and (3) hold, let $\bar{y}$ be any nonzero element of N/K and let u be arbitrary in N. Then $\bar{y} \neq \bar{0}$ implies y^2 is not in K, by (2). Thus the N-module yN is not contained in K. By Lemma 4.19, K + yN is an N-module. Since K + yN properly contains K, it follows from (1) that K + yN = N. Hence there is a k in K and an n in N such that u = k + yn, i.e., $\bar{u} = \overline{yn}$. By (3) then, there is an m in N such that $\bar{u} = \overline{my}$. This shows that both $\bar{u} = \bar{y}\ \bar{z}$ and $\bar{u} = \bar{z}\ \bar{y}$ have solutions in N/K, so the nonzero elements of N/K form a multiplicative group, i.e., N/K is a nearfield.

These characterizations (Theorem 5.14, Corollary 5.17, and Theorem 5.19) of the difference nearrings that are nearfields can be combined with Theorem 3.1 to characterize, in terms of the ideals of those theorems, the nearrings that have representations as subdirect sums of nearfields. For example, Theorem 5.14 yields

Theorem 5.20: A nonzero nearring N is isomorphic to a subdirect sum of nearfields if and only if the intersection of all bimodular m-maximal ideals of N is the zero ideal.

Proof: If N is isomorphic to a subdirect sum of the nearfields N_i, then there exist homomorphisms h_i of N onto N_i. Let K_i be the kernel of h_i. Then N/K_i is isomorphic to

the nearfield N_i, and so, by Theorem 5.14, each K_i is a bimodular m-maximal ideal of N. Theorem 3.1 says that for each nonzero element n of N there is some K_i such that n is not in K_i. Hence the intersection of all the K_i must be the zero ideal.

Conversely, if the intersection of all the bimodular m-maximal ideals K_i of N is the zero ideal, then each N/K_i is a nearfield, and the natural homomorphisms h_i of N onto N/K_i are such that each nonzero element of N has a nonzero image under some h_i. By Theorem 3.1, N has a representation as a subdirect sum of the nearfields N/K_i.

CHAPTER VI

OTHER RESULTS: PEIRCE DECOMPOSITION FOR NEARRINGS

A nearring N will be called the ordered sum of subnearrings Q_i of N, in symbols $N = \dot{+}\{Q_i \mid i \in I\}$ where the index set I is linearly ordered, if each nonzero element of N can be expressed uniquely as the ordered sum of a finite number of nonzero elements q_i such that q_i is in Q_i, the order of the sum being that of the index set I.

N is clearly an ordered sum if the additive group of N is isomorphic to the discrete direct sum of the additive groups of subnearrings Q_i. It follows that each discrete direct sum of nearrings, as defined in Chapter III, may be considered as an ordered sum. Indeed, it may be considered as such for each possible ordering of the summands.

There exist nearrings that are ordered sums, but that are not direct sums. For example, let S be an arbitrary ring, and let R be the usual extension ring of S such that R has an identity element and contains an ideal that is isomorphic to S. That is, let R be the set $\{(x,n) \mid x \in S, n \in Z\}$, where Z is the ring of integers, together with the operations defined by $(x,m)+(y,n) = (x+y,m+n)$ and $(x,m)(y,n) =$

$(xy+nx+my,mn)$, where (x,m) and (y,n) are arbitrary elements of R. It is clear that S is isomorphic to the ideal $S' = \{(x,0) \mid x \in S\}$, that Z is isomorphic to the subring $Z' = \{(0,n) \mid n \in Z\}$, and finally that $R = S' \dot{+} Z'$. The multiplication in R, however, is not the componentwise multiplication of the direct sum of the subrings S' and Z', and thus not every ordered sum is a direct sum.

Theorem 6.1: If e is an idempotent in the nearring N such that $0en = 0n$ for each n in N, then $N = Q \dot{+} R = R \dot{+} Q$, where $Q = \{en \mid n \in N\}$ and $R = \{r \in N \mid er = 0r = 0\}$.

Proof: Certainly each element n of N has the two representations $n = en + (-en + n)$ and $n = (n - en) + en$, where the element en is in Q, and, under the hypothesis that $0en = 0n$, both $(n - en)$ and $(-en + n)$ are in R. Also, if t is in Q then $et = t$, and if t is in R then $et = 0$. Thus 0 is the only element Q and R have in common, and this implies the uniqueness of each of the two representations given above for an arbitrary element n of N. It remains to be shown only that Q and R are subnearrings of N.

Because the left distributive law holds in N, it is clear that Q is an additive group. Moreover, Q is a subnearring of N, for both $e(m - n) = em - en$ and $(em)(en) = e(men)$ are in Q for each m and n in N. Also, if r and s are in R, then

$$e(r - s) = er - es = 0, \text{ and } 0(r - s) = 0r - 0s = 0.$$

Thus R is an additive group. Finally,

$e(rs) = (er)s = 0s = 0$, and $0(rs) = (0r)s = 0s = 0$, so R is also a subnearring of N.

This is a modified version of a theorem in [4], where it is stated without the $0en = 0n$ hypothesis and without the condition that $0R = \{0\}$. The decomposition is still valid without these assumptions, but R cannot be shown to be a subnearring.

Two corollaries are immediate consequences of Theorem 6.1. The second of these is commonly known as the "Nearring Decomposition Theorem".

Corollary 6.2: If e is any idempotent in the special nearring N, then $N = Q \dot{+} R = R \dot{+} Q$, where $Q = eN = \{en \mid n \in N\}$ and $R = (0:e) = \{r \in N \mid er = 0\}$.

Proof: Because N is special, $0en = 0n$ and $0r = 0$ for each n and r in N.

Corollary 6.3: For each nearring N, $N = Q \dot{+} R = R \dot{+} Q$, where $Q = 0N$ and $R = (0:0)$.

Proof: Let $e = 0$ in Theorem 6.1.

A generalization of Theorem 6.1 replaces the single idempotent e by a set E of orthogonal idempotents. A set $E = \{e_i \mid i \in I\}$ of idempotents of a nearring N is said to be orthogonal if $e_i e_j = 0$ whenever $i \neq j$, where i and j are, of course, elements of the index set I. Any subset of an orthogonal set of idempotents is obviously orthogonal.

Let $E = \{e_i | i \in I\}$ be an orthogonal set of idempotents of a nearring N such that 0 is in E. Although it is not assumed that I is finite or denumerable, the positive integers Z^+ will be used as elements of a denumerable subset of I. Let $Q_i = \{e_i n | n \in N\}$, and let $R_i = \{r \in N | e_i r = 0r = 0\}$.

Since E is orthogonal and contains 0, the condition $0e_i n = 0n$ of Theorem 6.1 holds for each e_i in E. It follows that $N = Q_i \dot{+} R_i$ for each i in I. Moreover, all elements of E other than e_i are in R_i. Thus each R_i is a nearring that contains an orthogonal set E_i of idempotents such that $0er = 0r$ for each r in R and each e in E_i, and hence Theorem 6.1 can be applied again to decompose R_i.

More specifically, choose e_1 and e_2 in E. Then $N = Q_1 \dot{+} R_1$, and $R_1 = \{e_2 r | r \in R_1\} \dot{+} \{r \in R_1 | e_2 r = 0r = 0\}$. But $\{e_2 r | r \in R_1\} = R_1 \cap Q_2$, and $\{r \in R_1 | e_2 r = 0r = 0\} = R_1 \cap R_2$. Thus $N = Q_1 \dot{+} R_1 \cap Q_2 \dot{+} R_1 \cap R_2$. Again, all elements of E except e_1 and e_2 are seen to be in $R_1 \cap R_2$, and Theorem 6.1 can be applied to $R_1 \cap R_2$. In this manner, with the aid of the Axiom of Choice, a denumerable subset of E can be selected such that $N = \dot{+}\{S_i | i \in Z^+\} \dot{+} S_\infty$, where $S_\infty = \cap\{R_i | i \in Z^+\}$, $S_1 = Q_1$, $S_2 = R_1 \cap Q_2$, $S_3 = R_1 \cap R_2 \cap Q_3$, and in general, $S_k = \cap \{R_i | i = 1, 2, \cdots, k-1\} \cap Q_k$. Of course, if E is itself finite or denumerably infinite, the elements $e_1, e_2, e_3, \cdots$ can be so chosen that E is exhausted after a finite or denumerable number of steps.

In this decomposition, if N is a special nearring, then

$Q_i = \{0\}$ when $e_i = 0$. Also, it may happen that S_∞ (or $\cap \{R_i | i\varepsilon I\}$ if E is finite) contains only the element 0. These two observations, together with the fact that the elements $e_1, e_2, e_3, \cdots$ can be chosen in arbitrary order from E, essentially complete the proof of

Theorem 6.4: Let $E = \{e_i | i\varepsilon I\}$ be an orthogonal set of idempotents of a nearring N such that 0 is in E. For each i in I let $Q_i = \{e_i n | n\varepsilon N\}$, and let $R_i = \{r\varepsilon N | e_i r = 0r = 0\}$. Then for each denumerable subset I' of I, $N = \dot{+}\{S_i | i\varepsilon I'\} \dot{+} S_\infty$, where $S_\infty = \cap \{R_i | i\varepsilon I'\}$ is a right ideal of N, $S_1 = Q_1$, $S_2 = R_1 \cap Q_2$, and in general $S_k = \cap \{R_i | i=1,2,\cdots,k-1\} \cap Q_k$. If E is a finite set of k elements, then N has (k+1)!, k!, or (k-1)! such decompositions, according as none, one, or both of Q' and S_{k+1} are $\{0\}$, where $Q' = Q_i$ such that $e_i = 0$ and $S_{k+1} = \cap \{R_i | i=1,2,\cdots,k\}$.

Proof: The only claim not yet established is that S_∞ (or S_{k+1} if E is finite with k elements) is a right ideal. But each R_i is, by definition, just the intersection of the annihilator right ideal of 0 with that of e_i, and the intersection of right ideals is again a right ideal.

As an example, let G be the additive group having three elements, $G = \{0,1,2\}$ with the addition modulo 3 as the group operation, and let N be the nearring of all transformations of G into itself. Each element of N will be represented by a triple, the triple (abc) representing the transformation

that takes 0 into a, 1 into b, and 2 into c. As usual, right hand notation is used for transformations. Thus (0)(102) = 1, (1)(102) = 0, (2)(102) = 2.

Let $e_1 = (000)$, $e_2 = (010)$, and $e_3 = (002)$. It is clear that these elements are orthogonal idempotents and that e_1 is the zero of N. A simple computation shows that

$$Q_1 = \begin{Bmatrix}(000)\\(111)\\(222)\end{Bmatrix}, \quad Q_2 = \begin{Bmatrix}(000)(101)(202)\\(010)(111)(212)\\(020)(121)(222)\end{Bmatrix}, \quad Q_3 = \begin{Bmatrix}(000)(110)(220)\\(001)(111)(221)\\(002)(112)(222)\end{Bmatrix},$$

$$R_1 = \begin{Bmatrix}(000)(010)(020)\\(001)(011)(021)\\(002)(012)(022)\end{Bmatrix}, \quad R_2 = \begin{Bmatrix}(000)\\(001)\\(002)\end{Bmatrix}, \quad R_3 = \begin{Bmatrix}(000)\\(010)\\(020)\end{Bmatrix},$$

$$S_1 = \begin{Bmatrix}(000)\\(111)\\(222)\end{Bmatrix}, \quad S_2 = \begin{Bmatrix}(000)\\(010)\\(020)\end{Bmatrix}, \quad S_3 = \begin{Bmatrix}(000)\\(001)\\(002)\end{Bmatrix}, \quad S_4 = \{(000)\}.$$

By Theorem 6.4 then, $N = S_1 \dot{+} S_2 \dot{+} S_3$.

No characterization is known for those nearrings, such as the one in the preceding example, that have a finite set of k orthogonal idempotents for which $S_{k+1} = \{0\}$. Certainly, the nearring of all transformations of a given finite group into itself possesses such a set; it is the set of those transformations that map one element onto itself and all other elements onto the identity element. To see that not every nearring having such a finite set of orthogonal idempotents is of this form, consider the additive group of integers modulo 4. The set of those transformations of this group into itself that map 3 onto either 3 or 0 forms a proper subnearring of the full transformation nearring of the group, and yet this subnearring and the full transforma-

tion nearring have the same set of orthogonal idempotents.

The set $C = \{x \in N \mid xn = nx \text{ for each } n \in N\}$ is called the (multiplicative) center of N and an element x in C is called a central element. The center C of N may well be empty, and even if nonempty it may not be a subnearring of N, (see [4]). An element x in the (left) nearring N is called distributive if $(n + m)x = nx + mx$ for each n and m in N.

The assumption that central orthogonal idempotent elements exist in a nearring is, of course, a strong one, albeit surely weaker than the assumption that multiplication is commutative. Several of the implications of such an assumption are brought together in the next theorem.

Theorem 6.5: If $E = \{e_1, e_2, \cdots\}$ is a set of central orthogonal idempotents in the nearring N, then

(1) N is special if 0 is in E or if E has two or more elements.

(2) Each e_i in E is distributive in N.

(3) $T = \{t \in N \mid e_i t = 0 \text{ for each } e_i \text{ in } E\}$ is an ideal of N.

(4) Any finite sum of distinct e_i from E is idempotent.

(5) Each n in N is distributive modulo T over any finite sum of distinct e_i from E. That is, $(\Sigma e_i)n - \Sigma e_i n$ is in T for each n in N.

(6) If 0 is in E or if E has two or more elements, then $\overline{E} = \{0 + T\} \cup \{e_i + T \mid e_i \in E\}$ is a set of central orthogonal idempotents in N/T such that $\{\overline{t} \in N/T \mid \overline{e_i}\,\overline{t} = \overline{0} \text{ for each } \overline{e_i}$

in $\overline{E}\} = \{\overline{0}\}$.

(7) If 0 is in E or if E has two or more elements, each n + T in N/T is distributive over any finite sum of distinct e_i + T.

Proof: (1) If 0 is central, then $0n = n0 = 0$ for each n in N, so N is special. If E has more than one element, then $e_i \neq e_j$ implies $0n = e_ie_jn = ne_ie_j = n0 = 0$, so 0 is central and N is special.

(2) Each central element is distributive.

(3) T, being the intersection of the annihilator right ideals of the e_i, is known to be a right ideal of N. For each t in T, n in N, and e_i in E

$$e_i(nt) = (e_in)t = (ne_i)t = n(e_it) = n0 = 0.$$

Thus $NT \subseteq T$, so T is an ideal of N.

(4) Let Σe_i be any finite sum of distinct e_i from E. Then $(\Sigma e_i)^2 = (\Sigma e_j)(\Sigma e_i) = \Sigma(\Sigma e_j)e_i = \Sigma e_i^2 = \Sigma e_i$.

(5) With Σe_i as in (4), let $x = (\Sigma e_i)n - \Sigma e_in$. Then $e_jx = 0$ for each e_j in E, so x is in T.

(6) Assume 0 is in E or E has two or more elements. By (1), N is special. Let $\overline{x} = x + T$. Then $\overline{0}\ \overline{e_i} = \overline{0e_i} = \overline{0} = \overline{e_i0} = \overline{e_i}\ \overline{0}$ for each e_i in E. It is a matter of similarly trivial calculation to show that $\overline{E}$ is a set of central orthogonal idempotents in N/T. If $\overline{e_i}\ \overline{n} = \overline{0}$ for each e_i in E, then e_in is in T for each e_i in E, so $0 = e_i(e_in) = e_i^2n = e_in$ for each e_i in E. Thus if $\overline{n}$ is in $\overline{T} = \{\overline{t} \in N/T \mid \overline{e_i}\ \overline{t} = \overline{0}$ for each $\overline{e_i}$ in $\overline{E}\}$, then n is in T, so $\overline{T} = \{\overline{0}\}$.

(7) By (5), applied to N/T, $(\Sigma\overline{e_i})\overline{n} - \Sigma\overline{e_i}\ \overline{n}$ is in $\overline{T}$. By (6), $\overline{T} = \{\overline{0}\}$, so the proof is complete.

LIST OF REFERENCES

1. Barnes, Wilfred E. Introduction to Abstract Algebra. Boston: D. C. Heath and Company, 1963.

2. Beidleman, James C. "A radical for near-ring modules," Michigan Mathematical Journal, 12 (1965), pp. 377-383.

3. _____. "Quasi-regularity in near-rings," Mathematische Zeitschrift, 89 (1965), pp. 224-229.

4. Berman, Gerald and Silverman, Robert J. "Near-rings," American Mathematical Monthly, 66 (1959), pp. 23-24.

5. Betsch, Gerhard. "Ein Radikal für Fastringe," Mathematische Zeitschrift, 78 (1962), pp. 86-90.

6. Blackett, D. W. "Simple and semisimple near-rings," Proceedings of the American Mathematical Society, 4 (1953), pp. 772-785.

7. Deskins, W. E. "A radical for near-rings," Proceedings of the American Mathematical Society, 5 (1954), pp. 825-827.

8. Dickson, L. E. "On finite algebras," Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, (1905), pp. 358-393.

9. Jacobson, N. Structure of Rings. Providence: American Mathematical Society Colloquium Publications, Vol. 37, revised edition, 1964.

10. Kalscheuer, F. "Die Bestimmung aller stetigen Fastkörper, über dem Körper der reelen Zahlen als Grundkörper," Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 13 (1940), pp. 413-435.

11. Laxton, R. R. "Primitive distributively generated near-rings," Mathematika, 8 (1961), pp. 142-158.

12. _____. "A radical and its theory for distributively generated near-rings," Journal of the London Mathematical Society, 38 (1963), pp. 40-49.

13. _____. "Prime ideals and the ideal-radical of a distributively generated near-ring," Mathematische Zeitschrift, 83 (1964), pp. 8-17.

14. McCoy, N. H. The Theory of Rings. New York: The Macmillan Company, 1964.

15. Neumann, B. H. "On the commutativity of addition," Journal of the London Mathematical Society, 15 (1940), pp. 203-208.

16. van der Walt, A. P. J. "Prime ideals and nil radicals in near-rings," Archiv der Mathematik, 15 (1964), pp. 408-414.

17. Zassenhaus, H. "Über endliche Fastkörper," Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 11 (1936), pp. 187-220.