THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

STRUCTURE THEORY FOR GENERALIZED p-RINGS

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

GENE LEVY

Norman, Oklahoma

1955

STRUCTURE THEORY FOR GENERALIZED p-RINGS

A THESIS

APPROVED FOR THE DEPARTMENT OF MATHEMATICS

BY

Albert A. Grau

John E. [illegible]

R. V. Andree

[illegible]

[illegible]

ACKNOWLEDGMENT

I wish to express my deep appreciation to Professor Albert A. Grau for his kind assistance in the preparation of this thesis, and to the members of the Thesis Committee for their helpful suggestions and criticisms.

TABLE OF CONTENTS

Chapter		Page
I.	INTRODUCTION...........................	1
II.	THE q-RINGS...........................	5
III.	RESTRICTED q-RINGS....................	16
IV.	SOME REMARKS ON A THEOREM OF WADE'S....	30
V.	COMMUTATIVE, ASSOCIATIVE, AND DISTRIBUTIVE FUNCTIONS ON (3,3)-RINGS..........................	35
LIST OF REFERENCES...........................		44

CHAPTER I

INTRODUCTION

This paper is chiefly concerned with the structure of a certain class of rings. In 1936 Stone [1] started the movement in this direction in a paper containing a representation theorem for Boolean rings. In 1937 McCoy and Montgomery [2] published a paper containing a representation theorem for a more general class of rings than the Boolean rings. In the intervening years several results have been obtained by others which aid in amplifying these original results. The best compilation of these results is in a book by McCoy [3] which appeared in 1948.

Before proceeding it might be well to review the definitions of Boolean rings and p-rings and to state some of the principal results contained in aforementioned papers.

<u>Definition 1.1</u>: A Boolean ring is a ring R such that, if $x \in R$, then $x^2 = x$.

Some of the results obtained by Stone are:

<u>Theorem 1.1</u>: If R is a Boolean ring, R is commutative.

<u>Theorem 1.2</u>: If R is a Boolean ring, $2x = 0$ for all $x \in R$.

Before stating the representation theorem of Stone it should be mentioned that the symbol I_p will be used for the ring of the residue classes of the integers modulo p.

Theorem 1.3: If R is a Boolean ring, then R is isomorphic to a direct sum of the rings I_2.

McCoy and Montgomery characterize a generalized Boolean ring, or a p-ring, in the following manner:

Definition 1.2: A p-ring is a ring R such that $x^p = x$ for all $x \in R$ and $p\,x = 0$ for all $x \in R$.

Some of the results obtained by McCoy and Montgomery are:

Theorem 1.4: If R is a p-ring, then R is commutative.

Theorem 1.5: If R is a p-ring, then R is isomorphic to a subdirect sum of the rings I_p.

In this paper a larger class of rings is studied. While it is too much to hope that in the more general case the results will be as precise as those listed previously, surprisingly good results are obtained.

In Chapter II we introduce the concept of a q-ring. It is shown that every q-ring is isomorphic to a subdirect sum of Galois fields. Within certain slight limitations, the converse is also shown to be true. Necessary and sufficient conditions for the existence of a q-ring are determined. At the end of the chapter examples are given to show that structurally it is very difficult to differentiate between q-rings.

In Chapter III the idea of a (q,c)-ring is advanced. The connection between q and c is fully explored, culminating in the formulation of conditions both necessary and sufficient for the existence of these rings. Representation theorems for the rings are obtained. While there remain certain ambiguities about the structure of such rings, theorems are obtained which enable one to tell for a certain q and c which Galois fields must be included in a representation of the rings and which fields may be included in a representation of some rings with that particular q and c, but not included in a representation of other rings with the same q and c. Examples are given to clarify the theorems at the end of the chapter.

In this chapter considerable space is devoted to a study of those rings for which $q = c$. A conjecture is advanced, and some results are obtained. In the near future the author hopes to be able to prove or disprove the conjecture.

In Chapter IV attention is directed to a recent paper by Wade [4]. In this paper the concept of a p-ring is generalized; the rings are then connected with Post algebras. It is demonstrated that many of the rings studied by Wade are actually (q,c)-rings.

In Chapter V attention once again returns to the original paper by Stone. The center of attraction at this time is the rather remarkable operations, often called logical sum and logical product, which enable him to construct Boolean algebras from Boolean rings. These operations have the unusual property of being mutually distributive. It is shown that for the 3-ring the only operation which is mutually distributive with multiplication is one which transforms everything into zero. The commutative, associative functions such that multiplication distributes over them are determined. In conclusion, the commutative, associative functions which distribute over addition are also ascertained.

CHAPTER II

THE q-RINGS

Since the q-ring is a generalization of the p-ring and Boolean ring, we shall first recall the definition of those rings and point out some of the considerations which led to this particular generalization.

A Boolean ring R is a ring of more than one element with the additional property that, for all $x \in R$, $x^2 = x$. From this it follows that, for all $x \in R$, $2x = 0$, and R is commutative.

McCoy and Montgomery [2] formulated the concept of a p-ring as a ring R of more than one element such that, for all $x \in R$, (1) $x^p = x$, and (2) $p\,x = 0$. It is to be noted that (2) does not follow from (1) as in the case of the Boolean ring. The remark should be also inserted that when $p > 2$, (2) has the effect of eliminating the Boolean ring as a trivial example of a p-ring.

<u>Definition 2.1</u>: A ring R of more than one element is called a q-ring, $q \geq 2$, if

(1) $x^q = x$ for all $x \in R$, and

(2) if $1 < t < q$, then there is a $x \in R$ such that $x^t \neq x$.

An equivalent formulation of (2) which will be used at various times is

(2') If there exists an $r > 1$ such that $x^r = x$ for all $x \in R$, then $r \geqq q$.

A more natural generalization of the p-ring might appear to be one obtained by replacing (2) by

(3) $qx = 0$ for all $x \in R$.

However, there is still an open question as to whether or not the class of rings having properties (1) and (3) includes any rings other than the p-rings. Some results in this connection appear in Chapter III.

While it was deemed necessary to discard (3), it was imperative that some restriction be included to eliminate various trivial examples of q-rings. (2) accomplishes this; thus, a Boolean ring can not also be a 4-ring.

We shall call q the degree of the ring.

In our investigation of the q-rings we shall depend quite heavily on a theorem due to Jacobson [5] and two theorems due to Birkhoff [6]. These theorems follow.

Theorem 2.1 (Jacobson): If for every element x in a ring R there exists a positive integer n (x) such that $x^{n(x)} = x$, then R is commutative.

Theorem 2.2 (Birkhoff): Every ring is isomorphic to a subdirect sum of subdirectly irreducible rings.

Theorem 2.3 (Birkhoff): Every subdirectly irreducible commutative ring without non-zero nilpotent elements is a field.

It should be mentioned that the only elementary proofs of Theorem 2.1 are due to Herstein [7], [8]. In the first paper Herstein offers an elementary proof that R is commutative when n is constant; in the last paper he offers an elementary proof of the more general theorem. Forsythe and McCoy [9] offer an elementary proof in the case n is a prime, while Kaplansky [10] has been able to prove commutativity in a slightly more general case.

Definition 2.2: The characteristic of a ring R is the least positive integer c such that $cx = 0$ for all $x \varepsilon R$; if no such positive integer exists, we say that the characteristic is infinite.

We first show that the characteristic of a q-ring is finite.

Lemma 2.1: If R is a q-ring, the characteristic c of R is a divisor of $n^q - n$.

Proof: Let $x \varepsilon R$. Then $nx \varepsilon R$, and $(nx)^q = nx$. That is, $n^q x^q - nx = n^q x - nx = (n^q - n)\, x = 0$. Hence, the characteristic is a divisor of $n^q - n$.

This raises the question as to whether or not, for a fixed q, every divisor of $2^q - 2$ is the characteristic of some q-ring. While we as yet have no basis for an answer, it is a consequence of Theorem 3.1 that such is not the case. Some examples will be given at that time.

It follows from Theorem 2.2 that every q-ring is isomorphic to a subdirect sum of subdirectly irreducible rings, each of which has the property that, for all $x \in R$, $x^q = x$. Then, by Theorem 2.1, these rings are commutative, and, by Theorem 2.3, these rings are actually fields, since these rings can have no non-zero nilpotent elements. It can easily be shown that these fields are actually the Galois fields.

<u>Lemma 2.2</u>: A field F all of whose elements satisfy the equation $x^q = x$, contains not more than q elements.

Proof: Let $p(x) = x^q - x$. Every element in F is a root of the equation $p(x) = 0$, and has associated with it a linear factor of $p(x)$. Let $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_r$ be the elements of F. Then $(x - \alpha_1)$, $(x - \alpha_2)$, ..., $(x - \alpha_r)$ are factors of $p(x)$. Let $f(x) = (x - \alpha_1) \; (x - \alpha_2) \; \ldots \; (x - \alpha_r)$. Then $p(x) = g\,(x)f(x)$. Since $f(x)$ is of degree r and $p(x)$ of degree q, it follows that $r \leqq q$.

<u>Theorem 2.4</u>: A subdirectly irreducible q-ring is a Galois field.

Proof: This follows immediately from Lemmas 2.1 and 2.2 and the discussion preceeding Lemma 2.2.

We now see that if R is a subdirectly irreducible q-ring, then $q = p^n$ for some p and some positive integer n.

If R is a q-ring or even a ring with property (1), definition 2.1, and $x \in R$, the element x^{q-1} has properties both interesting and useful in obtaining later results. We shall now establish some of these properties. To simplify the notation we shall place $e_x = x^{q-1}$.

<u>Lemma 2.3</u>: If R is a ring with property (1) and $x \in R$, then $e_x x = x$.

Proof: $e_x x = x^{q-1} \cdot x = x^q = x$.

<u>Lemma 2.4</u>: If R is a ring with property (1) and $x \in R$, then $e_x^n = e_x$, $n = 1,2,3,\ldots$.

Proof: This can be proved by induction. First,

$$e_x^2 = (x^{q-1})^2 = x^{2q-2} = x^q \cdot x^{q-2} = x \cdot x^{q-2} = x^{q-1} = e_x.$$

Assume true when $n = k$. Then,

$$e_x^{k+1} = e_x^k \cdot e_x = e_x \cdot e_x = e_x.$$

<u>Lemma 2.5</u>: If R is a ring with property (1) and $x \in R$, then $e_x^n x = x$, $n = 1, 2, 3, \cdots$.

Proof: This follows at once from Lemmas 2.3 and 2.4.

<u>Lemma 2.6</u>: If R is a ring with property (1) and $x \in R$, then $e_x^n x^m = x^m$, $n = 1,2,3,\cdots$, $m = 1,2,3,\cdots$.

Proof: Lemma 2.5 establishes this for the case $m = 1$. When $m > 1$, we have

$$e_x^n x^m = e_x^n (x \cdot x^{m-1}) = (e_x^n x) x^{m-1} = x \cdot x^{m-1} = x^m.$$

<u>Lemma 2.7</u>: If R is a q-ring, there is an element $x \in R$ such that if $x^r = x$, then $r-1 = n(q-1)$ for some positive integer n.

Proof: The definition of a q-ring assures us that there is an element $x \in R$ such that $x^q = x$, but $x^t \neq x$, $1 < t < q$.

Let

$$r-1 = n(q-1) + b, \quad b < q-1.$$

Then

$$x^r = x^{r-1}\cdot x = x^{n(q-1)+b}\cdot x = x^{n(q-1)}\cdot x^b \cdot x = e_x^n x^{b+1} = x^{b+1} = x.$$

Since $b+1<q$, this is impossible unless $b+1=1$. Thus, $r-1=n(q-1)$, and the lemma is established.

Lemma 2.8: If R is a q-ring and $x \varepsilon R$, then

$$x^{nq-(n-1)} = x, \quad n = 1,2,3,\cdots.$$

Proof: By Lemma 2.5 we have

$$e_x^n \cdot x = x, \quad n = 1,2,3,\cdots.$$

But $e_x = x^{q-1}$, so we have

$$(x^{q-1})^n \cdot x = x^{nq-n}\cdot x = x^{nq-n+1} = x^{q-(n-1)} = x.$$

We are now in a position to prove a theorem which plays an important role in ascertaining the structure of q-rings.

Theorem 2.5: If R is a q-ring, every non-trivial homomorph R' of R is a q'-ring with $q'=2$ or $q \equiv 1 \pmod{(q'-1)}$.

Proof: From the definition of homomorphism $x' \varepsilon R'$ implies that $x'^q = x'$. Yet it may also be true that $x'^{q'} = x'$, $1<q'<q$, for all $x' \varepsilon R'$. If there are q_1, q_2, q_3, ..., q_n, $1<q_i<q$, $i=1,2, \ldots n$, with this property, let

$$q' = \min(q_1, q_2, \cdots, q_n).$$

Otherwise, $q'=q$. If $q'=2$, it is clear that R' is a Boolean ring. If $q'>2$, then there is an element $y \varepsilon R'$ such that $y^{q'} = y$, but $y^t \neq y$ if $1<t<q'$. Let $q = r(q'-1)+s$, $0 \leq s < q'-1$.

$$y^q = y^{r(q'-1)+s} = (y^{q'-1})^r \cdot y^s = (e_y)^r \cdot y^s = y^s = y.$$

Since $s < q'$, and $y^t \neq y$, $1 < t < q'$, it must be true that $s = 1$. Hence, $q = r(q'-1) \neq 1$, and $q \equiv 1 \pmod{(q'-1)}$.

It was established in Lemma 2.1 that the characteristic of a q-ring is finite. A more important result concerning the characteristic follows.

Theorem 2.6: If R is a q-ring, the characteristic of R contains no repeated prime factors.

Proof: From Theorems 2.2 and 2.4 we know that every q-ring is isomorphic to a subdirect sum of Galois fields. The characteristic of a Galois field is a prime. The characteristic of a subdirect sum of Galois fields is the least common multiple of the characteristics of the Galois fields, that is, the least common multiple of a set of prime numbers. Hence, the characteristic of R will contain no repeated prime factors.

In view of the rather severe restrictions thus imposed on the characteristic of a q-ring, one might naturally ask if there is a ring of degree q for every positive q. That such is not the case is proved in the following theorem.

Theorem 2.7: If R is a q-ring, then either $q = 2$ or there exists a prime p and a positive integer n such that $q \equiv 1 \pmod{(p^n-1)}$.

Proof: By Theorem 2.2 we know that R is isomorphic to a subdirect sum of subdirectly irreducible rings. This isomorphism establishes a natural homomorphism between R and the subdirectly irreducible rings. From Theorem 2.5

we learn that these rings are also q-rings. If the degree of R is greater than two, then the degree of at least one of the subdirectly irreducible rings must be greater than two, for the subdirect sum of a set of rings of degree two is of degree $\leqq$ two. Let T be the ring of degree q', $q' > 2$. Then, by Theorem 2.5, $q \equiv 1 \pmod{(q'-1)}$. According to Theorem 2.4 T is actually a Galois field; hence, there exists a prime p and a positive integer n such that $q' = p^n$. Consequently,

$$q \equiv 1 \pmod{(p^n - 1)}.$$

While this may appear to be a relatively weak restriction on q, it eliminates as possible values of q such numbers as 6, 12, and 14.

Naturally it is desirable to determine conditions both necessary and sufficient for the existence of a q-ring. Before we can do this, however, it is necessary to prove a theorem which is not only essential to this task but is also of considerable interest in its own right.

Theorem 2.8: The subdirect sum R of the Galois fields $GF\,p_1^{\alpha_{11}}, \ldots, GF\,p_1^{\alpha_{1m_1}}, GF\,p_2^{\alpha_{21}}, \ldots, GF\,p_2^{\alpha_{2m_2}}, \ldots, GF\,p_n^{\alpha_{n1}}, \ldots, GF\,p_n^{\alpha_{nm_n}}$, $p_i^{\alpha_{ij}} \neq p_k^{\alpha_{kl}}$ if $i \neq k$ or $j \neq l$, is a q-ring with $q = 1 + \operatorname{lcm}(p_1^{\alpha_{11}} - 1, \ldots, p_1^{\alpha_{1m_1}} - 1, p_2^{\alpha_{21}} - 1, \ldots, p_2^{\alpha_{2m_2}} - 1, \ldots, p_n^{\alpha_{n1}} - 1, \ldots, p_n^{\alpha_{nm_n}} - 1)$ and with characteristic $c = p_1 p_2 \cdots p_n$.

Proof: That the subdirect sum of a set of Galois fields is a ring is well-known. We shall now show that it is a q-ring. Let $x \in R$. Then $x = (x_{11}, \ldots, x_{1m_1}, x_{21}, \ldots,$

$x_{2m_2}, \ldots, x_{n1}, \ldots, x_{nm_n}$), $x_{ij} \varepsilon GF p_i^{\alpha_{ij}}$. Since $x_{ij} \varepsilon GF p_i^{\alpha_{ij}}$, $x_{ij}^{p_i^{\alpha_{ij}}-1} = e_{x_{ij}}$. Let $q-1 = \text{lcm}\,(p_1^{\alpha_{11}}-1, \ldots, p_1^{\alpha_{1m_1}}-1, p_2^{\alpha_{21}}-1, \ldots, p_2^{\alpha_{2m_2}}-1, \ldots, p_n^{\alpha_{n1}}-1, \ldots, p_n^{\alpha_{nm_n}}-1) = \gamma_{ij}(p_i^{\alpha_{ij}}-1)$. Then $x_{ij}^{q-1} = x_{ij}^{\gamma_{ij}(p_i^{\alpha_{ij}}-1)} = (x_{ij}^{p_i^{\alpha_{ij}}-1})^{\gamma_{ij}}$ $(e_{x_{ij}})^{\gamma_{ij}} = e_{x_{ij}}$. Hence, $x_{ij}^q = x_{ij}^{q-1} \cdot x_{ij} = e_{x_{ij}} \cdot x_{ij} = x_{ij}$. So $x^q = (x_{11}^q, \ldots, x_{1m_1}^q, x_{21}^q, \ldots x_{2m_2}^q, \ldots, x_{n1}^q, \ldots, x_{nm_n}^q) = (x_{11}, \ldots, x_{1m_1}, x_{21}, \ldots, x_{2m_2}, \ldots, x_{n1}, \ldots, x_{nm_n}) = x$. To show that R is a q-ring we need to show that condition (2') also holds.

By Lemma 2.7 there exists an element $y_{ij} \varepsilon GF p_i^{\alpha_{ij}}$ such that if $y_{ij}^r = y_{ij}$ then $r-1 = n_{ij}(p_i^{\alpha_{ij}}-1)$. Let $z_{ij} = (\ldots, y_{ij}, \ldots)$ and $z^r = z$ for all $z \varepsilon R$. Then $y_{ij}^r = y_{ij}$ and $r-1 = \gamma_{ij}(p_i^{\alpha_{ij}}-1)$, $i = 1,2, \ldots, n$, $j = 1,2, \ldots, n$. Hence, $r-1 \geqq \text{lcm}\,(p_1^{\alpha_{11}}-1, \ldots, p_1^{\alpha_{1m_1}}-1, p_2^{\alpha_{21}}-1, \ldots, p_2^{\alpha_{2m_2}}-1, \ldots, p_n^{\alpha_{n1}}-1, \ldots, p_n^{\alpha_{nm_n}}-1) = q-1$, and $r \geqq q$. Consequently, R is a q-ring.

Let $m = p_1 p_2 \cdots p_n$. There exists an element $y_{ij} \varepsilon GF p_i^{\alpha_{ij}}$ such that $p_i y_{ij} = 0$, but $r\, y_{ij} \neq 0$ if $r < p_i$. Let $x_{ij} = (\ldots, y_{ij}, \ldots) \varepsilon R$ and let the characteristic of R be c. If $cx_{ij} = 0$, then $c\, y_{ij} = 0$, and $c \doteq \lambda_i p_i$, $i = 1,2, \ldots, n$. Hence, $c = \lambda p_1 p_2 \cdots p_n \geqq m$.

Let $x = (x_{11}, \ldots, x_{1m_1}, x_{21}, \ldots, x_{2m_2}, \ldots, x_{n1}, \ldots, x_{nm_n}) \varepsilon R$. Then $mx = (mx_{11}, \ldots, mx_{1m_1}, mx_{21}, \ldots,$

$mx_{2n_2}, \ldots, mx_{n1}, \ldots, mx_{nn_n}) = (0, 0, \ldots, 0) = 0$. Accordingly, $c \leqq m$.

Thus, $c = m$.

Conditions both necessary and sufficient for a ring R to be a q-ring can now be established.

<u>Theorem 2.9</u>: There is a ring of degree q if and only if

$$q = 1 + \underset{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1), \quad p_i^{\alpha_{ij}} \neq p_k^{\alpha_{kl}}$$

if $i \neq k$ or $j \neq l$.

Proof: Let $q = 1 + \underset{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1)$.

We wish to show that there is a ring of degree q. Let R be the direct sum of the Galois fields $GFp_i^{\alpha_{ij}}$, $i = 1,2,\ldots, n$, $j = 1,2,\ldots, n_i$. By Theorem 2.8 this direct sum is a q-ring with

$$q = 1 + \underset{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1)$$

Let R be a q-ring. Then by Theorems 2.2 and 2.4 R is isomorphic to a subdirect sum of Galois fields, $GFp_i^{\alpha_{ij}}$, $i = 1,2,\ldots,n$, $j = 1,2,\ldots,n_i$. Without loss of generality we can assume that $p_i^{\alpha_{ij}} \neq p_k^{\alpha_{kl}}$ if $i \neq k$ or $j \neq l$, since the repetition of a Galois field affects neither the characteristic or degree of the ring. Hence, by Theorem 2.8, $q = 1 + \underset{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1)$.

At the conclusion of Theorem 2.7 we cited several numbers which could not serve as possible values of q. We can now add other numbers to this list. For example, 10 was not eliminated as a possible value of q by Theorem 2.7, but it is eliminated by Theorem 2.9.

While the results obtained in this chapter give some insight into q-rings, a few examples will suffice to show that the actual structure of the rings is rather indefinite. To illustrate, $13 = 1 + \text{lcm}\ (7-1, 5-1)$, $13 = 1 + \text{lcm}\ (13-1, 4-1)$, and $13 = 1 + \text{lcm}\ (13-1, 3-1)$. That is, one can construct a q-ring, $q = 13$, as the subdirect sum of GF_7 and GF_5, or as the subdirect sum of GF_{13} and GF_4, or as the subdirect sum of GF_{13} and GF_3. The previous remarks are not intended to exhaust the possible means of constructing q-rings, $q = 13$, but only to mention a few. From these we can see that the actual structure of the rings may differ quite widely.

It is of interest to note that the characteristic of the first ring is 35, the characteristic of the second is 52, and the characteristic of the third is 39. This would seem to indicate that consideration of both the degree and the characteristic of a ring is essential to any attempt to study the structure of these rings. The results obtainable in this fashion comprise the major portion of Chapter III.

CHAPTER III

RESTRICTED q-RINGS

We first define some of the terms used in this chapter.

Definition 3.1. A (q,c)-ring is a q-ring of characteristic c.

If there exists a ring of degree q and characteristic c, q will be said to belong to c.

Two results obtained in Chapter II are important in establishing relationships between q and c. By Lemma 2.1 we find that c must be a divisor of $2^{q} - 2$. By Theorem 2.6 we find that c is the product of distinct primes. We are now in a position to prove a more restrictive relationship between q and c.

Theorem 3.1. If q belongs to $c = p_1 p_2 p_3 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$, then either $p_i = 2$, and/or there are positive integers $\alpha_i \geqq 1$ such that $q \equiv 1 \pmod{p_i^{\alpha_i} - 1}$, $i = 1, 2, \ldots, n$.

Proof: Let R be a (q,c)-ring, $c = p_1 p_2 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$. By Theorems 2.2 and 2.4 we know that R is isomorphic to a subdirect sum of Galois fields, and, by

Theorem 2.8, that the characteristic of R is the least common multiple of the characteristics of the Galois fields. Hence, there must be at least one Galois field of characteristic p_1 in this subdirect sum, at least one of characteristic p_2, and at least one of characteristic p_i. Let $GF p_i^{\alpha_i}$ be the Galois field of characteristic p_i. The isomorphism between R and the subdirect sum of Galois fields establishes a homomorphism between R and $GF p_i^{\alpha_i}$. If $p_i^{\alpha_i} > 2$, then, by Theorem 2.5, $q \equiv 1 \pmod{p_i^{\alpha_i} - 1}$; if $p_i^{\alpha_i} = 2$, then $p_i = 2$, and the theorem is established.

Following Lemma 2.1 we raised the question of whether or not every divisor of $2^q - 2$ was the characteristic of some ring of degree q. We can now cite some examples which show that such is not the case. For, let $q = 4$. Then $2^q - 2 = 14$. 7 is a divisor of 14. Yet there is no (4,7)-ring, since $4 \not\equiv 1 \pmod 6$. However, all the results that we have obtained thus far do not enable us to answer questions about the existence of certain (q,c)-rings. To raise one: Is there a (5,6)-ring? 6 is a divisor of $2^5 - 2$, and $5 \equiv 1 \pmod 2$. Every condition imposed by Lemma 2.1, Theorem 2.6, and Theorem 3.1 has thus been satisfied. Despite this, we have no assurance that there is a (5,6)-ring. The next theorem establishes necessary and sufficient conditions for the existence of a (q,c)-ring; these conditions eliminate the possibility of a (5,6)-ring.

<u>Theorem 3.2.</u> q belongs to $c = p_1 p_2 p_3 \cdots p_n$, $p_i \neq p_j$

when $i \neq j$, if and only if there exist $\alpha_{ij} \geqq 1$ such that

$$q = 1 + \operatorname*{lcm}_{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}} (p_i^{\alpha_{ij}} - 1).$$

Proof: Let $q = 1 + \operatorname*{lcm}_{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}} (p_i^{\alpha_{ij}} - 1)$.

Let R be the direct sum of the fields $GF_{p_i^{\alpha_{ij}}}$. From Theorem 2.8, we know that R is a q-ring with

$$q = 1 + \operatorname*{lcm}_{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}} (p_i^{\alpha_{ij}} - 1).$$

and $c = p_1 p_2 \ldots p_n$. Hence, q belongs to c.

Let R be a (q,c)-ring. Then, as before, R is isomorphic to a subdirect sum of Galois fields $GF_{p_i^{\alpha_{ij}}}$. Again using Theorem 2.8 we find that

$$q = 1 + \operatorname*{lcm}_{\substack{i=1,2,\ldots,N \\ j=1,2,\ldots,N_i}} (P_i^{\alpha_{ij}} - 1)$$

and $c = P_1 P_2 \ldots P_N$, $P_K \neq P_L$ if $K \neq L$. Since $c = p_1 p_2 \ldots p_n$, we have

$$p_1 p_2 \cdots p_n = P_1 P_2 \ldots P_N$$

Since p_i is a divisor of $P_1 P_2 \ldots P_N$, there is a $P_K = p_i$. Conversely, since P_L is a divisor of $p_1 p_2 \ldots p_n$, there is a $p_j = P_L$. Hence, the primes P_i are just those primes p_i, $i = 1,2,3,\ldots, n$, which are the factors of c. Thus we have shown that if q belongs to $c = p_1 p_2 \ldots p_n$, there exist $\alpha_{ij} \geqq 1$ such that

$$q = 1 + \operatorname*{lcm}_{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,n_i}} (p_i^{\alpha_{ij}} - 1).$$

<u>Corollary 3.1:</u> If q belongs to $c = p_1 p_2 p_3 \ldots p_n$,

then $q \geqq 1 + \operatorname{lcm}(p_1 - 1, p_2 - 1, p_3 - 1, \ldots, p_n - 1)$.

Proof: It follows immediately from Theorem 3.2 that the minimal q which belongs to c is that for which $\alpha_{ij} = 1$ for all i and j, i.e., $1 + \operatorname{lcm}(p_1 - 1, p_2 - 1, p_3 - 1, \ldots, p_n - 1)$.

We now see that there can be no (5,6)-ring since there do not exist α_{ij} such that

$$5 = 1 + \operatorname{lcm}(3^{\alpha_{1j_1}} - 1,\ 2^{\alpha_{2j_2}} - 1), \quad j_i = 1, 2, \cdots, n_i$$

In Chapter II we raised the question of rings whose degree and characteristic are equal. We know there are such rings, for the p-rings of McCoy and Montgomery [2] have this property. It is the conjecture of the author that there are no other rings with this property, but the question is still open. A partial answer follows.

All rings whose degree q and characteristic c are equal have the following properties:

(1) $q = p_1 p_2 p_3 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$,

(2) $p_1 p_2 p_3 \cdots p_n = 1 + \operatorname{lcm}(p_i^{\alpha_{ij}} - 1)$, $\quad i = 1, 2, \cdots, n$; $j = 1, 2, \cdots, n_i$

(3) q is a divisor of $2^q - 2$.

<u>Lemma 3.1</u>: If $n > 1$, then $\operatorname{lcm}(p_1 - 1, p_2 - 1, \ldots, p_n - 1) < p_1 p_2 p_3 \cdots p_n - 1$.

Proof: $\operatorname{Lcm}(p_1 - 1, p_2 - 1, \ldots, p_n - 1) \leqq (p_1 - 1)(p_2 - 1) \cdots (p_{n-1} - 1)(p_n - 1) < p_1 p_2 \cdots p_{n-1}(p_n - 1) = p_1 p_2 \cdots p_n - p_1 p_2 \cdots p_{n-1} < p_1 p_2 \cdots p_n - 1$.

<u>Lemma 3.2:</u> If $p_1 \neq p_2$, then $p_1 p_2 - 1 \neq \text{lcm}\,(p_1^{\alpha_1 j_1} - 1,$
$j_i = 1, 2, \cdots, n_i$
$p_2^{\alpha_2 j_2} - 1)$.

Proof: Assume there exist α_{ij} such that $p_1 p_2 - 1 = \text{lcm}\,(p_1^{\alpha_1 j_1} - 1, p_2^{\alpha_2 j_2} - 1)$. Since $p_1 - 1$ divides $p_1^{\alpha_1 j_1} - 1$, it divides $p_1 p_2 - 1$. Likewise, $p_2 - 1$ divides $p_1 p_2 - 1$. Hence,

$$(1) \quad p_1 p_2 \equiv 1 \ (\text{mod}(p_1 - 1)),$$
$$(2) \quad p_1 p_2 \equiv 1 \ (\text{mod}(p_2 - 1)).$$

The above can be written in the following form

$$(1') \quad p_2 \equiv 1 \ (\text{mod}(p_1 - 1)),$$
$$(2') \quad p_1 \equiv 1 \ (\text{mod}(p_2 - 1)).$$

From these we obtain

$$(3) \quad p_2 = 1 + r\,(p_1 - 1),$$
$$(4) \quad p_1 = 1 + s\,(p_2 - 1).$$

These lead us to

$$p_2 = \frac{p_1 - 1}{s} + 1 = 1 + r\,(p_1 - 1).$$

Hence,

$$\frac{p_1 - 1}{s} = r\,(p_1 - 1),$$
$$p_1 - 1 = rs(p_1 - 1),$$
$$1 = rs.$$

But r and s are both positive integers, so that $r = s = 1$. Consequently, we find that $p_1 = p_2$ in contradiction, and the lemma is established.

<u>Lemma 3.3:</u> If $n > 1$ and there is an i such that $p_i = 2$, then

$$p_1\, p_2\, p_3 \cdots p_n \neq 1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1)$$

Proof: For definiteness assume that $p_1 = 2$. Then $p_1\, p_2\, p_3 \cdots p_n$ is even. Since $p_i \neq p_j$ if $i \neq j$, then p_2 will be odd and $p_2^{\alpha_{2j}}$ will be odd. Accordingly, $p_2^{\alpha_{2j}} - 1$ will be even, and

$$1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1)$$

will be odd. This proves the lemma.

Hardy and Wright [11] list only 6 composite numbers q less than 2,000 which are divisors of $2^q - 2$. These are 341, 561, 645, 1387, 1729, and 1905. Each of these can be eliminated as a possible value of the degree and characteristic of a ring by one of the preceding lemmas or by showing directly that it can not be written in the form

$$p_1\, p_2 \cdots p_n = 1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1).$$

We now know that if there is a (q,q)-ring, q composite, that q must be greater than 2,000, that it must be the product of at least three odd primes, and, furthermore, that in the representation of q as

$$1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} - 1)$$

at least one of the α_{ij} is greater than one.

An example will show that the technique used in proving Lemma 3.2 is inadequate in the general case. Let

$p_1 = 5$, $p_2 = 17$, and $p_3 = 13$. Then $p_1\ p_2\ p_3\ -1$ is divisible by $p_1\ -1$, $p_2\ -1$, and $p_3\ -1$. By considering all α_{ij} such that $p_i^{\alpha_{ij}} < p_1\ p_2\ p_3\ -1$, it can be shown that there are no α_{ij} such that $p_1\ p_2\ p_3\ -1 = \underset{\substack{i=1,2,3\\ j=1,2,\cdots,n_i}}{\mathrm{lcm}}\ (p_i^{\alpha_{ij}}\ -1)$.

We are at present left in the position of neither being able to prove that there is no (q,q)-ring, q composite, nor being able to exhibit such a ring.

Definition 3.2: If q belongs to c, the c-maximal divisor set of (q-1) is the set of all divisors of (q-1) of the form $p_i^{\alpha_i}\ -1$, p_i a prime factor of c.

Note that Theorem 3.2 assures us that there is at least one divisor of q-1 of the form $p_i^{\alpha_i}\ -1$ for each prime factor of c.

Definition 3.3: A subdirect sum T of Galois fields is a representation of a (q,c)-ring R if T is isomorphic to R.

Definition 3.4: A Galois field $GFp_i^{\alpha_i}$ is a component of a (q,c)-ring R if there exists a representation of R which includes $GFp_i^{\alpha_i}$.

Definition 3.5: The Galois field $GFp_i^{\alpha_i}$ is an essential component of a (q,c)-ring R if every representation of R includes $GFp_i^{\alpha_i}$.

Lemma 3.4: If $GFp_i^{\alpha_{ij}}$ is a component of a (q,c)-ring, then $c = \lambda p_i$.

Proof: Let R be a (q-c)-ring with $GFp_i^{\alpha_{ij}}$ as a component. Then R is isomorphic to a subdirect sum of Galois fields, $GFp_1^{\alpha_{11}}$, ..., $GFp_1^{\alpha_{1m_1}}$, ..., $GFp_i^{\alpha_{i1}}$, ..., $GFp_i^{\alpha_{ij}}$, ..., $GFp_i^{\alpha_{im_i}}$, ..., $GFp_m^{\alpha_{m1}}$, ..., $GFp_m^{\alpha_{mn_m}}$, $GFp_k^{\alpha_{kl}} \neq GFp_m^{\alpha_{mn}}$ if $k \neq m$ or $l \neq n$. Hence, by Theorem 2.8, $c = p_1 \, p_2 \cdots p_i \cdots p_m = \lambda p_i$.

Lemma 3.5: If $GFp_i^{\alpha_{ij}}$ is a component of a (q,c)-ring, then $(p_i^{\alpha_{ij}} -1)$ is a member of the c-maximal divisor set of (q-1).

Proof: Let R be a (q,c)-ring with $GFp_i^{\alpha_{ij}}$ as a component. That is, R is isomorphic to a subdirect sum of Galois fields $GFp_1^{\alpha_{11}}$, ..., $GFp_1^{\alpha_{1m_1}}$, ..., $GFp_i^{\alpha_{i1}}$, ..., $GFp_i^{\alpha_{ij}}$, ..., $GFp_i^{\alpha_{im_i}}$, ..., $GFp_m^{\alpha_{m1}}$, ..., $GFp_m^{\alpha_{mn_m}}$. By Theorem 2.8, $q-1 = \mathrm{lcm}\,(p_1^{\alpha_{11}} -1, \ldots, p_1^{\alpha_{1m_1}} -1, \ldots, p_i^{\alpha_{i1}} -1, \ldots, p_i^{\alpha_{ij}} -1, \ldots, p_i^{\alpha_{im_i}} -1, \ldots, p_m^{\alpha_{m1}} -1, \ldots, p_m^{\alpha_{mn_m}} -1)$. By Lemma 3.4 p_i is a prime factor of c. Hence, $(p_i^{\alpha_{ij}} -1)$ is a member of the c- maximal divisor set of q-1.

Lemma 3.6: If q belongs to c, the least common multiple of the c- maximal divisor set of (q-1) is (q-1).

Proof: Let S be the c-maximal divisor set of q-1. The lcm $\{S\} \leqq$ q-1, since every member of S is a divisor of q-1.

Since q belongs to c, we have, from Theorem 3.2

$$q = 1 + \underset{\substack{i=1,2,\cdots,m \\ j=1,2,\cdots,m_i}}{\mathrm{lcm}} (p_i^{\alpha_{ij}} -1),$$

where p_i is a prime divisor of c. Hence, $(p_i^{\alpha_{ij}} -1) \varepsilon$ S, and

$$\operatorname{lcm}\{S\} \geqq \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\operatorname{lcm}} (p_i^{\alpha_{ij}} -1) = q-1.$$

Accordingly, $\operatorname{lcm}\{S\} = q-1$.

The preceding lemmas place us in position to develop our fundamental structure theorems. We shall first prove that every member of the c-maximal divisor set of (q-1) is a component of a (q,c)-ring.

<u>Theorem 3.3</u>: If $p_i^{\alpha_i} -1$ is a member of the c-maximal divisor set of (q-1), then $GFp_i^{\alpha_i}$ is a component of a (q,c)-ring.

Proof: Let $p_k^{\alpha_k} -1$ be a member of the c-maximal divisor set of (q-1). Since q belongs to $c = p_1 p_2 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$, then, following Theorem 3.2, there exist $\alpha_{ij} \geqq 1$ such that

$$q = 1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\operatorname{lcm}} (p_i^{\alpha_{ij}} -1).$$

It may be that $p_k^{\alpha_k} -1$ is included in the set $\{p_i^{\alpha_{ij}} -1\}$. If it is, let R be the subdirect sum of $GFp_i^{\alpha_{ij}}$. According to Theorem 2.8, R is a (q,c)-ring with

$$q = 1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\operatorname{lcm}} (p_i^{\alpha_{ij}} -1)$$

and $c = p_1 p_2 \cdots p_n$.

If $p_k^{\alpha_k} -1$ is not included in the set $\{p_i^{\alpha_{ij}} -1\}$, let R be the subdirect sum of $GFp_i^{\alpha_{ij}}$ and $GFp_k^{\alpha_k}$. Again using Theorem 2.8, R is a (q',c')-ring with

$$q' - 1 = \underset{\substack{i=1,2,\dots,n \\ j=1,2,\dots,n_i}}{\text{lcm}} (p_i^{\alpha_{ij}} - 1, p_k^{\alpha_k} - 1) = \text{lcm}\ (q-1,\ p_k^{\alpha_k} - 1)$$

$= q-1$. It also follows that $c' = p_1 p_2 \cdots p_n = c$. Hence, R is a (q,c)-ring. In either case, $GFp_k^{\alpha_k}$ is a component of a (q,c)-ring.

Of even more interest is the theorem which follows, dealing with the essential components of a (q,c)-ring. The representation theorems of Stone [1] and McCoy and Montgomery [2] are special cases of this theorem.

<u>Theorem 3.4</u>: GFp_i is an essential component of a (q,c)-ring if and only if p_i is a factor of c, $(p_i - 1)$ is a member of the c-maximal divisor set of (q-1), but $(p_i^{\alpha_i} - 1)$ is not a member if $\alpha_i > 1$.

Proof: Let S be the c-maximal divisor set of (q-1). Let $(p_i - 1) \varepsilon S$, but $(p_i^{\alpha_i} - 1) \not\varepsilon S$ if $\alpha_i > 1$. Since p_i is a factor of c, every representation of a (q,c)-ring must include a Galois field of characteristic p_i. Suppose some representation includes $GFp_i^{\alpha_i}$, $\alpha_i > 1$. Then, by Lemma 3.5, $(p_i^{\alpha_i} - 1)$ is a member of S in contradiction. Therefore, every representation will include GFp_i.

Let GFp_i be an essential component of a (q,c)-ring. Then $(p_i - 1) \varepsilon S$ and p_i is a factor of c. Suppose $(p_i^{\alpha_i} - 1) \varepsilon S$, $\alpha_i > 1$. Then, by Theorem 3.3, there is a (q,c)-ring R whose representation includes $GFp_i^{\alpha_i}$. Let the representation of R include $GFp_1^{\alpha_{11}}, \dots, GFp_i^{\alpha_i}, \dots, GFp_i, \dots, GFp_n^{\alpha_{nn_n}}$. Let T be the direct sum of all the fields appearing in the representation of R except GFp_i. Then T is a (q',c')-ring with $q'-1 = \text{lcm}\,(p_1^{\alpha_{11}}-1, \ldots, p_i^{\alpha_i}-1, \ldots, p_m^{\alpha_{mm}}-1) = \text{lcm}\,(p_1^{\alpha_{11}}-1, \ldots, p_i-1, \ldots, p_i^{\alpha_i}-1, \ldots, p_m^{\alpha_{mm}}-1) = q-1$ since p_i-1 is a divisor of $p_i^{\alpha_i}-1$. Also $c' = p_1 \cdots p_i \cdots p_n = c$. We have thus constructed a (q,c)-ring with a representation not including GFp_i in contradiction. Hence, $(p_i^{\alpha_i}-1) \notin S$, $\alpha_i > 1$.

Corollary 3.2: If q belongs to $c = p_1 p_2 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$, and p_i-1, $i = 1,2, \ldots, n$, is a member of the c-maximal divisor set of q-1, but $p_i^{\alpha_i}-1$, $\alpha_i > 1$, $i = 1,2, \ldots, n$, is not a member, then every (q,c)-ring is isomorphic to a subdirect sum of Galois fields GFp_i, $i = 1,2, \ldots, n$.

Proof: This follows immediately from the previous theorem.

The McCoy-Montgomery representation theorem, which includes the Stone representation theorem, is actually a special case of this corollary. The hypotheses of this theorem restrict the rings to those for which $q = c = p$ and the only member of the c-maximal divisor set is p-1. Accordingly, the rings are isomorphic to a subdirect sum of Galois fields GFp.

Theorem 3.5: $GFp_i^{\alpha_i}$, $\alpha_i > 1$, is an essential component of a (q,c)-ring if and only if p_i is a factor of c, $(p_i^{\alpha_i}-1)$ is a member of the c-maximal divisor set S of (q-1), and $\text{lcm}\,\{S-(p_i^{\alpha_i}-1)\} < q-1$.

Proof: Suppose $p_i^{\alpha_i}-1$ is a member of the c-maximal

divisor set S of (q-1) and lcm $\{S-(p_i^{\alpha_i}-1)\} < q-1$.
Suppose the representation of the (q,c)-ring R does not include $GFp_i^{\alpha_i}$, that is, R is isomorphic to a subdirect sum of Galois fields $GFp_i^{\alpha_i \gamma}$ which does not include $GFp_i^{\alpha_i}$. Then, by Theorem 2.8, the degree of R is

$$q' = 1 + \underset{\substack{i=1,2,\cdots,n \\ j=1,2,\cdots,n_i}}{\mathrm{lcm}} (p_i^{\alpha_i \gamma} - 1) \leqq 1 + \mathrm{lcm}\,\{S-(p_i^{\alpha_i}-1)\} < q$$

in contradiction. Hence, the representation of R must include $GFp_i^{\alpha_i}$.

Let R be a (q,c)-ring with $GFp_i^{\alpha_i}$ as an essential component. By Lemma 3.4, p_i is a factor of c, and, by Lemma 3.5, $(p_i^{\alpha_i}-1)$ is a member of the c-maximal divisor set S of (q-1). Lcm $\{S-(p_i^{\alpha_i}-1)\} \leqq$ lcm $\{S\} = q-1$. Suppose lcm $\{S-(p_i^{\alpha_i}-1)\} = q-1$. Since $(p_i^{\alpha_i}-1) \varepsilon S$ and (p_i-1) is a divisor of $(p_i^{\alpha_i}-1)$, $(p_i-1) \varepsilon S$. Let T be the direct product of the Galois fields $GFp_i^{\alpha_i \gamma}$ such that $(p_i^{\alpha_i \gamma}-1) \varepsilon \{S-(p_i^{\alpha_i}-1)\}$. Then, by Theorem 2.8, the degree q' of T is $q' = 1 +$ lcm $\{S-(p_i^{\alpha_i}-1)\} = q$. The characteristic of T is c, so T is a (q,c)-ring with a representation which does not include $GFp_i^{\alpha_i}$ in contradiction. Hence, lcm $\{S-(p_i^{\alpha_i}-1)\} < q-1$.

In view of Theorems 3.4 and 3.5, one might ask if there are any (q,c)-rings, q composite, whose structure is uniquely determined. The answer is yes. As an example, consider the (21,55)-ring. The c-maximal divisor set of 20 = 21-1 includes only 4 = 5-1, and 10 = 11-1. By Theorem 3.4,

GF_5 and GF_{11} are essential components of a (21,55)-ring; they are the only components, so every (21,55)-ring is isomorphic to a subdirect sum of the fields GF_5 and GF_{11} .

There remain other (q,c)-rings whose structure is not so definite. Consider the (25,195)-ring. The c-maximal divisor set of $24 = 25-1$ includes $2 = 3-1$, $8 = 3^2 - 1$, $4 = 5-1$, $24 = 25-1$, and $12 = 13-1$. An examination of Theorems 3.4 and 3.5 shows that the only essential component is GF_{13}. It is possible to exhibit (25,195)-rings which do not have a particular member of the set GF_3, GF_9, GF_5, and GF_{25} as a component. The direct sum of GF_5, GF_9, and GF_{13} is a (25, 195)-ring which does not have either GF_3 or GF_{25} as a component. The direct sum of GF_{25}, GF_3, and GF_{13} is a (25,195) ring which does not have either GF_5 or GF_9 as a component.

As an application of Theorem 3.5, let us examine a (25,39)-ring. The c-maximal divisor set of $24 = 25-1$ includes $2 = 3-1$, $8 = 3^2-1$, and $12 = 13-1$. Essential components of a (25,39)-ring are GF_9 and GF_{13}. There are some (25-39)-rings which include GF_3 as a component and others which do not include GF_3. The direct sum of GF_3, GF_9, and GF_{13} is an example of the former, while GF_9 and GF_{13} is an example of the latter.

In summary, it appears that there are essential ambiguities in the structure of many (q,c)-rings. We can say that in any representation of a particular (q,c)-ring only certain Galois fields may be used, but we can not guarantee that in every representation all permissible Galois fields will be used.

CHAPTER IV

SOME REMARKS ON A THEOREM OF WADE'S

Wade [4] considers a slightly more general class of rings than the p-rings, namely, commutative rings R with the following restrictions:

(A) There exists an integer m such that for $x \in R$, $mx = 0$.

It is not assumed that R necessarily has characteristic m. In that which follows p denotes any prime divisor of m, and p^{n} the maximum power of p dividing m.

(B) For every $x \in R$, there is a $y \in R$ such that $x^{p} - x = py$.

(C) If $px = 0$, there is a y such that $x = p^{n-1}y$.

We shall show in this chapter that, for certain values of m, commutative rings with properties (A), (B), and (C) are actually (q,c)-rings. To do this we consider a representation theorem obtained by Wade and prove that the rings used in this representation are (q,c)-rings.

Let I_m denote the residue class ring of the integers modulo m. Then the theorem of Wade's can be stated in the following form:

<u>Theorem 4.1</u> (Wade): A ring R with properties (A), (B), (C) is a subring of the direct sum of rings I_m.

We shall first restrict ourselves to dealing with the rings I_m, where m is the product of distinct primes. In order to establish that these rings are (q,c)-rings we need the following theorem.

<u>Theorem 4.2</u>: If $n = ar$, $m = br$, $(a,b) = 1$, $m = p_1 p_2 p_3 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$, $\alpha = \text{lcm}(p_1 - 1, p_2 - 1, \ldots, p_n - 1)$, then

$$n^{\alpha} \equiv 1 \pmod{b},$$

$$n^{\alpha+1} \equiv n \pmod{m}.$$

Proof: Since $m = p_1 p_2 p_3 \cdots p_n$, $p_i \neq p_j$ if $i \neq j$, and $m = br$, it follows that $(b,r) = 1$. Also, $(b,a) = 1$, so $(b,n) = 1$. Now, $b = p_1' p_2' \cdots p_m'$, where p_i', $i = 1,2, \ldots, m$, is one of the set $\{p_1, p_2, \ldots, p_n\}$. For convenience, arrange the factors $p_1, p_2, \ldots, p_m$ in such a manner that $b = p_1 p_2 \cdots p_m$ and $r = p_{m+1} \cdots p_n$. By Fermat's theorem

$$(1) \quad n^{p_i - 1} \equiv 1 \pmod{p_i}, \; i = 1,2,\ldots, m,$$

$$(2) \quad n^{\alpha} \equiv 1 \pmod{p_i}, \; i = 1,2,\ldots, m.$$

That is,

$$(3) \quad n^{\alpha} = 1 + l_i p_i, \; i = 1,2,\ldots,m,$$

$$(4) \quad n^{\alpha} = 1 + l\, p_1 p_2 p_3 \cdots p_m = 1 + l\, b.$$

Consequently,

$$(5) \quad n^{\alpha} \equiv 1 \pmod{b}.$$

If we multiply (4) by $n = ar$ we obtain

(6) $n^{\alpha+1} = n + 1 a m$,

(7) $n^{\alpha+1} \equiv n \pmod{m}$.

Corollary 4.1: If $(n,m) = 1$, $m = p_1 p_2 \ldots p_n$, $p_i \neq p_j$ if $i \neq j$, $\alpha = \text{lcm}(p_1 - 1, p_2 - 1, \ldots, p_n - 1)$, then

$$n^{\alpha} \equiv 1 \pmod{m}$$

Proof: This follows easily from Theorem 4.2, since we now have $r = 1$ and $m = b$.

We are now in a position to prove our assertion that, under certain restrictions, the rings I_m are (q,c)-rings.

Theorem 4.3: If $m = p_1 p_2 \ldots p_n$, $p_i \neq p_j$ if $i \neq j$, then the rings I_m are (q,c)-rings with $c = m$ and $q = 1 + \text{lcm}$ $(p_1 - 1, p_2 - 1, p_3 - 1, \ldots, p_n - 1)$.

Proof: That the integers modulo m form a ring is well known. Clearly the characteristic of the ring is m. If $n \in I_m$, from Theorem 4.2 we know that $n^q = n$, where $q = 1 +$ $\text{lcm}(p_1 - 1, p_2 - 1, p_3 - 1, \ldots, p_n - 1)$. Hence, I_m is a (q',c)- ring for some q'. It follows immediately from Corollary 3.1 that $q' \geqq q$; hence, I_m is a (q,c)-ring.

Let us replace property (A) of Wade by the following:

(A') There exists an integer $m = p_1 p_2 \ldots p_n$, $p_i \neq p_j$ if $i \neq j$, such that for $x \in R$, $mx = 0$.

We may now rewrite Theorem 4.1 as follows:

Theorem 4.4: A ring R with properties (A'), (B), (C), is a subring of the direct sum of (q,c)-rings with $c = m$ and $q = 1 + \text{lcm}(p_1 - 1, p_2 - 1, p_3 - 1, \ldots, p_n - 1)$.

Proof: This follows immediately from Theorems 4.1

and 4.3.

This leads to the following theorem.

Theorem 4.5: A ring R with properties (A'), (B), (C), is a (q,c)-ring with

$$m \equiv 0 \pmod{c},$$

$q = 2$ or $\text{lcm}\,(p_1 - 1, p_2 - 1, \ldots, p_n - 1) \equiv 0 \pmod{(q-1)}$.

Proof: The direct sum of (q,c)-rings is a (q,c)-ring. Hence, by Theorem 4.4, a ring R with properties (A'), (B), and (C) is a subring of a (q,c)-ring with $c = m$ and $q = 1 + \text{lcm}\,(p_1 - 1, p_2 - 1, \ldots, p_n - 1)$. A subring of a (q,c)-ring is another (q,c)-ring. Let c be the characteristic of the subring. Then we can write $m = rc + s$, where $s < c$. Let x be any element of the subring. Then $cx = 0$. Since x is an element of the original ring we also have

$$mx = (rc + s)x = rcx + sx = sx = 0.$$

This is impossible unless $s = 0$, hence

$$m \equiv 0 \pmod{c}.$$

Let q be the degree of the subring. If $q = 2$, we are through. If $q \neq 2$, then let x be any element of the subring. Then $x^q = x$. Since x is an element of the original ring we also have

$$x^{1 + \text{lcm}(p_1 - 1, p_2 - 1, \ldots, p_n - 1)} = x.$$

By Lemma 2.7

$$\text{lcm}\,(p_1 - 1, p_2 - 1, \ldots, p_n - 1) = n\,(q-1),$$

and

$$\text{lcm}\,(p_1 - 1, p_2 - 1, \ldots, p_n - 1) \equiv 0 \pmod{(q-1)}.$$

The next theorem illustrates the difficulty encountered when m is divisible by a power of a prime.

Theorem 4.6: If $m = p_1^{\alpha} p_2 \cdots p_n$, $\alpha > 1$, then
$p_1^{\beta} \not\equiv p_1 \pmod{m}$ for all $\beta > 1$.

Proof: Assume $p_1^{\beta} \equiv p_1 \pmod{m}$ for some $\beta > 1$. Then, $p_1^{\beta} - km = p_1$. Then, $p_1^{\beta-1} - kn = 1$, where $n = p_1^{\alpha-1} p_2 \cdots p_n$. Now, p_1 is a divisor of the left-hand side of this equation, and, consequently, p_1 must be a divisor of the right-hand side. But this is impossible, and the theorem is proven.

Corollary 4.2: If $m = p_1^{\alpha} p_2 \cdots p_n$, $\alpha > 1$, then the rings I_m are not (q,c)-rings.

Proof: Since $p_1^{\beta} \not\equiv p_1 \pmod{m}$ for all $\beta > 1$, there is no $q > 1$ such that, for all $x \in I_m$, $x^q = x$.

While the rings I_m are not (q,c)-rings, certain subrings are (q,c)-rings. If $m = p_1^{\alpha} p_2 \cdots p_n$, $\alpha > 1$, a ring having properties (A), (B), and (C), is then a subring of the direct sum of rings which are not (q,c)-rings. This subring, however, can be a (q,c)-ring. No results of general interest in this connection have been obtained.

CHAPTER V

COMMUTATIVE, ASSOCIATIVE, AND DISTRIBUTIVE FUNCTIONS ON (3,3)-RINGS

Initially, let us remark that a (3,3)-ring is in the notation of McCoy and Montgomery [2] a p-ring with $p=3$.

In his paper on Boolean algebras Stone [1] was able to start with a Boolean ring and, by introducing two new operations $\cup$, $\cap$ defined in terms of the ring operations, construct a Boolean algebra. Conversely, he was able to start with a Boolean algebra, define his ring operations in terms of the operations of the algebra, and construct a Boolean ring. In this manner he was able to establish an isomorphism between Boolean algebras and Boolean rings.

The two operations of the Boolean algebra are rather remarkable. Not only are they both commutative and associative, but they are also mutually distributive.

Jacobson also introduced a quasi-addition in his papers [12], [13] treating the structure of algebras and rings. Actually, this is the same operation Stone used in his study of Boolean algebras, but Jacobson uses it in connection with a wider class of rings.

This immediately raises the question: Is it possible to define on rings other than Boolean two operations each of which is commutative and associative and which are mutually distributive? In this chapter we answer that question for rings whose degree and characteristic are both 3.

Let us first recall the definitions of the operations of the Boolean algebra used by Stone:

$$a \cup b = a + b + ab,$$

$$a \cap b = a \cdot b.$$

Note that the algebraic "multiplication" is in no sense unusual, but that the "addition" is a little out of the ordinary.

Accordingly, we seek to determine the most general polynomial function having the following properties:

(A) $f(a,b) = f(b,a)$

(B) $f(a, f(b,c)) = f(f(a,b),c)$

(C) $a\, f(b,c) = f(ab,ac)$

(D) $f(a,bc) = f(a,b) \cdot f(a,c)$.

<u>Theorem 5.1</u>: A polynomial function defined on all (3,3)-rings and having properties (A), (B), (C), and (D) is identically zero.

Proof: The most general function possible is

(1) $f(a,b) = \lambda_1 a + \lambda_2 b + \lambda_3 ab + \lambda_4 a^2 + \lambda_5 b^2 + \lambda_6 a^2 b + \lambda_7 ab^2 + \lambda_8 a^2 b^2 + \lambda_9$.

From (C) it follows that $f(0,0) = 0 f(b,c) = 0$. But $f(0,0) = \lambda_9$, hence $\lambda_9 = 0$.

From (A) it follows that

(2) $\lambda_1(a-b)+\lambda_2(b-a)+\lambda_4(a^2-b^2)+\lambda_5(b^2-a^2)+\lambda_6(a^2b-ab^2)+\lambda_7(ab^2-a^2b)=0.$

This must hold when $a=1$, $b=0$. Thus we obtain

(3) $\lambda_1-\lambda_2+\lambda_4-\lambda_5=0.$

Likewise (2) must hold when $a=2$, $b=0$. This yields

(4) $2\lambda_1-2\lambda_2+\lambda_4-\lambda_5=0.$

Subtracting (4) from (3) one finds

$$\lambda_1=\lambda_2$$

Using this result in (3) leads to

$$\lambda_4=\lambda_5$$

(2) may now be written as

(5) $\lambda_6(a^2b-ab^2)+\lambda_7(ab^2-a^2b)=0.$

When $a=1$, $b=2$, it follows that

$$\lambda_6=\lambda_7$$

We now write (1) in the following form

(6) $f(a,b)=\lambda_1(a+b)+\lambda_3\,ab+\lambda_4(a^2+b^2)+\lambda_6(a^2b+ab^2)+\lambda_8a^2b^2.$

Using properties (A), (D), (A), and (D) in that order we find that $f(a^2,0)=f(0,a^2)=f(0,a)\cdot f(0,a)=f(a,0)\cdot f(a,0)=f(a,0)$.

However, $f(a^2,0)=\lambda_1a^2+\lambda_4a^2$, and $f(a,0)=\lambda_1a+\lambda_4a^2$. Hence,

(7) $\lambda_1a^2=\lambda_1a.$

When $a=2$, $\lambda_1=2\lambda_1$, and $\lambda_1=0$.

If we now use (C) we find that $af(a,0)=f(a^2,0)$. As a consequence,

(8) $\lambda_4 a = \lambda_4 a^2$.

As before, when $a = 2$, $2\lambda_4 = \lambda_4$, and $\lambda_4 = 0$.

Using (C) once again we have $af(a,b) = f(a^2, ab)$.

Accordingly,

(9) $\lambda_3(a^2b - ab) = \lambda_8(a^2b^2 - ab^2)$.

If $a = 2$, $b = 2$, it follows that $\lambda_3 = -\lambda_8$.

It is now possible to write (6) as

(10) $f(a,b) = \lambda_3(ab - a^2b^2) + \lambda_6(a^2b + a\ b^2)$.

Another use of (C) leads to

(11) $\lambda_3(c\ a\ b - c\ a^2b^2 - abc^2 + a^2b^2c^2) = 0$.

When $a = 1$, $b = 2$, $c = 2$, we find that $\lambda_3 = 0$.

Using only the demands that the operations be commutative and that the operations be mutually distributive, we have found that the function must be of the following form

(12) $f(a,b) = \lambda_6(a^2b + a\ b^2)$.

Use of (D) at this time yields

(13) $\lambda_6(a^2bc + ab^2c^2) = \lambda_6^2(a^2bc + abc^2 + ab^2c + a^2b^2c^2)$.

If $a = b = 2$, $c = 1$, we find that $\lambda_6 = 0$.

This proves the theorem.

May we again emphasize that in the above proof we did not demand that the function be associative.

Having failed in our quest for an "addition" which would be distributive with respect to "multiplication", we now seek to determine those functions which have properties (A), (B), and (C). These properties are those of ordinary addition, so we know that there is at least one such function.

There may be others. This search leads to the following theorem.

<u>Theorem 5.2</u>: The only non-zero polynomial functions on (3,3)-rings having properties (A), (B), and (C), are

$$f(a,b) = a + b,$$

and $$f(a,b) = 2a^2 b + 2ab^2.$$

Proof: Using those results of Theorem 5.1 which depend only on (A) and (C), we find that it is possible to write.

(1) $f(a,b) = \lambda_1(a+b) + \lambda_3 ab + \lambda_4(a^2 + b^2) + \lambda_6(a^2 b + ab^2) + \lambda_8 a^2 b^2.$

As before it follows from (C) that $af(a,0) = f(a^2,0)$. This yields

(2) $\lambda_4 a = \lambda_4 a^2.$

When $a = 2$, $2\lambda_4 = \lambda_4$, $\lambda_4 = 0$.

We now write

(3) $f(a,b) = \lambda_1(a+b) + \lambda_3 ab + \lambda_6(a^2 b + ab^2) + \lambda_8(a^2 b^2).$

$af(1,-1) = f(a,-a)$ by use of (C). Therefore,

(4) $a(-\lambda_3 + \lambda_8) = -\lambda_3 a^2 + \lambda_8 a^2.$

When $a = 2$, $\lambda_8 = \lambda_3$.

Again rewriting $f(a,b)$ we have

(5) $f(a,b) = \lambda_1(a+b) + \lambda_3(ab + a^2 b^2) + \lambda_6(a^2 b + ab^2).$

Use of (C) again leads to $af(1,1) = f(a,a)$. This yields

(6) $2\lambda_3 a = 2\lambda_3 a^2.$

If $a = 2$, $\lambda_3 = 2\lambda_3$, $\lambda_3 = 0$.

The last result enables us to write

(7) $f(a,b) = \lambda_1(a+b) + \lambda_6(a^2b + ab^2)$.

We now use (B) to obtain

$$f(a,\ \lambda_1(b+c) + \lambda_6(b^2c + bc^2)) = f(\lambda_1(a+b) + \lambda_6(a^2b+ab^2), c).$$

That is,

$$\lambda_1(a + \lambda_1(b+c) + \lambda_6(b^2c + bc^2)) + \lambda_6\{[a^2(\lambda_1(b+c) + \lambda_6(b^2c+bc^2)] + a[\lambda_1^2(b^2 + 2bc + c^2) + 2\lambda_1\lambda_6(2bc + 2b^2c^2) + \lambda_6^2(2b^2c^2 + 2bc)]\} = \lambda_1[\lambda_1(a+b) + \lambda_6(a^2b + ab^2) + c] + \lambda_6\{[\lambda_1^2(a^2 + 2ab + b^2) + 2\lambda_1\lambda_6(2ab + 2a^2b^2) + \lambda_6^2(2ab + 2a^2b^2)]c + [\lambda_1(a+b) + \lambda_6(a^2b + ab^2)]c^2\}.$$

This in turn gives

$$\lambda_1 a + \lambda_1^2(b+c) + \lambda_1\lambda_6(b^2c + bc^2) + \lambda_1\lambda_6(a^2b + a^2c) + \lambda_6^2(a^2b^2c + a^2bc^2) + \lambda_1^2\lambda_6(ab^2 + 2abc + ac^2) + 2\lambda_1\lambda_6^2(2abc + 2ab^2c^2) + \lambda_6(2ab^2c^2 + 2abc) = \lambda_1^2(a+b) + \lambda_1\lambda_6(a^2b + ab^2) + \lambda_1 c + \lambda_1^2\lambda_6(a^2c + 2abc + b^2c) + 2\lambda_1\lambda_6^2(2abc + 2a^2b^2c) + \lambda_6(2abc + 2a^2b^2c) + \lambda_1\lambda_6(ac^2 + bc^2) + \lambda_6^2(a^2bc^2 + ab^2c^2).$$

Simplification of above leads to

(8) $$\lambda_1 a + \lambda_1^2 c + \lambda_1\lambda_6(b^2c + a^2c) + \lambda_6^2 a^2b^2c + \lambda_1^2\lambda_6(ab^2 + ac^2) + 2\lambda_1\lambda_6^2(2ab^2c^2) + \lambda_6(2ab^2c^2) = \lambda_1^2 a + \lambda_1\lambda_6(ab^2 + ac^2) + \lambda_1 c + \lambda_1^2\lambda_6(a^2c + b^2c) + 2\lambda_1\lambda_6^2(2a^2b^2c) + \lambda_6(2a^2b^2c) + \lambda_6^2(ab^2c^2).$$

If we place $a=1$, $b=c=0$, we find

(9) $$\lambda_1 = \lambda_1^2 .$$

We use this result to write (8) as

(10) $$\lambda_6^2 a^2b^2c + \lambda_1\lambda_6^2 ab^2c^2 + 2\lambda_6 ab^2c^2 = \lambda_6^2 ab^2c^2 + \lambda_1\lambda_6^2 a^2b^2c + 2\lambda_6 a^2b^2c .$$

If we now let $a=2$, $b=c=1$, we obtain

(11) $$\lambda_6^2 - \lambda_1\lambda_6^2 + \lambda_6 = 0 .$$

The simplest (3,3)-ring is the ring of the residue classes of the integers modulo 3. If we select λ_1 and λ_6 from the elements of this ring, the values of λ_1 which satisfy (9) are 1 and 0. If $\lambda_1 = 1$, we find from (11) that $\lambda_6 = 0$. If $\lambda_1 = 0$, then $\lambda_6^2 + \lambda_6 = 0$ and $\lambda_6 = 2$. Thus the only functions having the desired properties are

$$f(a,b) = a + b,$$
$$f(a,b) = 2a^2 b + 2ab^2.$$

We had hoped that the above investigation would lead us to a "quasi-addition" having properties both interesting and useful. However, the only alternative to ordinary addition has a rather serious defect-namely, the "quasi-sum" of any element and zero is zero. This makes further study uninteresting.

There yet remains the possibility of generalizing the concept of "multiplication". Accordingly, we seek those polynomial functions having properties (A), (B), and

$$\text{(E)} \quad f(a,b+c) = f(a,b) + f(a,c).$$

Ordinary multiplication has these three properties, but there may be other functions having these properties.

<u>Theorem 5.3</u>: On (3,3)-rings the only polynomial function having properties (A), (B), and (E) is

$$f(a,b) = \lambda ab.$$

Proof: We again start with the most general function possible, namely

(1) $f(a,b) = \lambda_1 a + \lambda_2 b + \lambda_3 ab + \lambda_4 a^2 + \lambda_5 b^2 + \lambda_6 a^2 b + \lambda_7 ab^2 + \lambda_8 a^2 b^2 + \lambda_9$.

From (E) we obtain $f(a,0) = f(a,0) + f(a,0)$ and $f(a,0) = 0$. This leads to

(2) $\lambda_1 a + \lambda_4 a^2 + \lambda_9 = 0$.

If we place $a = 0$, $\lambda_9 = 0$.

Placing $a = 1$, we find $\lambda_1 + \lambda_4 = 0$.

Placing $a = 2$, we find $2\lambda_1 + \lambda_4 = 0$.

As a result, $\lambda_1 = \lambda_4 = 0$.

Using (A) and (E) yields $f(0,b) = f(b,0) = 0$.

Hence,

(3) $\lambda_2 b + \lambda_5 b^2 = 0$.

Placing $b = 1$ results in $\lambda_2 + \lambda_5 = 0$. Placing $b = 2$ gives $2\lambda_2 + \lambda_5 = 0$. Consequently, $\lambda_2 = \lambda_5 = 0$.

We now use (E) to obtain

$$\lambda_3 a(b+c) + \lambda_6 a^2(b+c) + \lambda_7 a(b^2 + 2bc + c^2) + \lambda_8 a^2(b^2 + 2bc + c^2)$$
$$= \lambda_3 ab + \lambda_6 a^2 b + \lambda_7 ab^2 + \lambda_8 a^2 b^2 + \lambda_3 ac + \lambda_6 a^2 c + \lambda_7 ac^2 + \lambda_8 a^2 c^2.$$

This reduces to

(4) $2\lambda_7 abc + 2\lambda_8 a^2 bc = 0$.

If in (4) we let $a = b = c = 1$, we find $2\lambda_7 + 2\lambda_8 = 0$. If we let $a = 2$, $b = c = 1$, we find $\lambda_7 + 2\lambda_8 = 0$. Consequently, $\lambda_7 = \lambda_8 = 0$.

The results obtained enable us to write

(5) $f(a,b) = \lambda_3 ab + \lambda_6 a^2 b$.

(A) says that $f(a,-a) = f(-a,a)$. This is used to obtain

(6) $2\lambda_6 a = 0$.

Placing $a = 2$ in (6) yields $\lambda_6 = 0$. Hence,

(7) $f(a,b) = \lambda_3 ab$.

Again it is of interest to note that the proof of this theorem in no place uses the demand that our function be associative.

We have shown in this chapter that it is impossible to parallel the concepts of logical sum and logical product in (3,3)-rings. If one retains the idea of ordinary multiplication, then addition must be defined in the usual sense or in a trivial fashion; if the idea of ordinary addition is retained, then one must define multiplication as usual or as a multiple thereof.

LIST OF REFERENCES

1. M. H. Stone, The theory of representations for Boolean Algebras, Transactions of the American Mathematical Society, Vol. 40 (1936), pp. 37-111.

2. N. H. McCoy and D. Montgomery, A representation of generalized Boolean rings, Duke Mathematical Journal, Vol. 3 (1937), pp. 455-459.

3. N. H. McCoy, Rings and Ideals, Baltimore, 1948.

4. L. I. Wade, Post Algebras and rings, Duke Mathematical Journal, Vol. 12 (1945), pp. 389-395.

5. N. Jacobson, Structure theory for algebraic algebras of bounded degree, Annals of Mathematics, Vol. 46 (1945), pp. 695-707.

6. G. Birkhoff, Subdirect unions in universal algebras, Bulletin of the American Mathematical Society, Vol. 50 (1944), pp. 764-768.

7. I. N. Herstein, A generalization of a theorem of Jacobson, American Journal of Mathematics, Vol. 73 (1951), pp. 756-762.

8. I. N. Herstein, A generalization of a theorem of Jacobson, American Journal of Mathematics, Vol. 75 (1953), pp. 105-111.

9. A. Forsythe and N. H. McCoy, On the commutativity of certain rings, Bulletin of the American Mathematical Society, Vol. 52 (1946), pp. 523-526.

10. I. Kaplansky, Commutativity of generalized Boolean rings, (Abstract) Bulletin of the American Mathematical Society, Vol. 51 (1945), p. 60.

11. Hardy and Wright, Theory of Numbers, Oxford, 1938.

12. N. Jacobson, Structure Theory of simple rings without finiteness assumptions, Transactions of the American Mathematical Society, Vol. 57 (1945), pp. 228-245.

13. N. Jacobson, <u>The radical and semi-simplicity for arbitrary rings</u>, <u>American Journal of Mathematics</u>, <u>Vol. 67</u> (1945), pp. 300-320.