AN INVESTIGATION OF RINGS PROPERLY CONTAINING FIELDS

A Thesis

Presented to

the Department of Mathematics

The Kansas State Teachers College of Emporia

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

by

Terrence Joseph Ryan

May 1970

Marion P. Emerson
Approved for the Major Department

Laurence C. Boylan
Approved for the Graduate Council

ACKNOWLEDGEMENTS

The writer wishes to express his appreciation to Dr. Marion P. Emerson for his early suggestions and patience, to Associate Professor Lester Laird for help in organizing and editing this material, and to his parents for their patience and understanding throughout the preparation of this paper.

T. J. R.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

I. RINGS AND FIELDS

Two of the more common mathematical structures studied in elementary abstract algebra are rings and fields.

A ring must form a commutative group under an operation called addition, and a second operation called multiplication must be closed, associative, and distributive with respect to addition. These properties are the minimal requirements for a ring.

A ring that, in addition to the above properties, contains a unity element is called a ring with unity. Because it is a well established fact that a ring without unity can always be considered to be contained in a ring with unity, rings in this paper will be, for the most part, rings with unity.

If multiplication is commutative and each nonzero element of the ring has a multiplicative inverse, the ring is called a field. In other words, a field is an additive commutative group that is also a multiplicative commutative group.

It should be obvious that a field is always a ring, but a ring is not necessarily a field. When referring to a ring that might contain a field, it is to be understood that the ring is not itself a field.

II. STATEMENT OF THE PROBLEM

There are rings that contain fields. Consider the ring Z/(6) of integers modulo 6. A straightforward argument will verify that the subset

$$\{0_6, 2_6, 4_6\}$$

is a field with unity 4_6.

Other rings do not contain fields. In the ring Z/(9) of integers modulo 9, the only proper subset that forms a commutative group under addition is the subset

$$\{0_9, 3_9, 6_9\}.$$

This set is not a field since $(3_9)(6_9) = 0_9$ proves that 3_9 and 6_9 are proper divisors of zero. A field has no proper divisors of zero.

It should be possible to determine which rings contain fields and which do not. Chapter II will be an investigation of this conjecture. In Chapter III, a brief examination will be made of multiplicative inverses in rings containing fields.

III. BASIC CONCEPTS

It is assumed that the reader has knowledge of the basic concepts of the theory of groups, rings, and fields. However, in this section, some of the basic concepts necessary for an understanding of this presentation will be reviewed.

Definition 1.1. A set S of one or more elements of a ring R is called an ideal in R if and only if it has the following properties:

(1) If a and b are in S, then a-b is in S.

(2) If a is in S, then, for all r in R, ar and ra are in S.[4, p. 52]

Definition 1.2. Let R and R' be rings. A mapping $w:R \longrightarrow R'$ of R into R' is called a (ring) homomorphism if, for any r and s in R,

$$w(r+s) = wr+ws, \quad w(rs) = (wr)(ws).$$

If, for any r' in R', wr = r' for some r in R, then w is said to be a homomorphism of R onto R'. If, also, wr = ws implies that r = s, then w is an isomorphism of R onto R'.[1, p. 89]

If $w:R \longrightarrow R'$ is a (ring) homomorphism, R has unity e, and r is any element of R, then

$$(we)(wr) = w(er) = wr$$

implies that R' will have unity e' = we.

Definition 1.3. If w is a homomorphism of the ring R into the ring R', the set

$$N = \left\{ r \text{ in } R \middle| wr = 0_{R'} \right\}$$

is called the kernel of w.[1, p. 90]

These first few definitions are particularly needed to understand the following important theorem in the theory of rings.

Theorem 1.4. (Fundamental Homomorphism Theorem for Rings). If N is an ideal of the ring R, then the mapping $w:R \longrightarrow R/N$, defined by $wr = r+N$, is a homomorphism of R onto R/N with kernel N. Conversely, if v is a homomorphism of R onto a ring R', then R' is isomorphic to R/K, where K is the kernel of v.[1, p. 90]

Definition 1.5. Let R be an arbitrary ring, r a fixed element of R, and Z the ring of integers. If n is an element of Z, the natural multiples of r are the integral multiples of r defined as follows. For n greater than 0,

$$nr = (r+r+r+---+r)_{n \text{ terms}}$$

and

$$(-n)r = n(-r).$$

For n equal to 0,

$$0r = 0_R.$$

Definition 1.6. If r is an element of a ring R, the additive subgroup generated by r is the set of all natural multiples of r. The order of this group is the number of elements it contains.

Theorem 1.7. For each ring R with unity $1'$, there is exactly one homomorphism $u:Z \longrightarrow R$.

Proof. Each homomorphism $w:S \longrightarrow S'$ of rings, as a homomorphism of additive groups, is a homomorphism of natural multiples, in the sense that

$$w(ns) = n(ws)$$

for all s in S and all integers n. In particular, since $we = e'$, it follows that

$$w(ne) = n(we) = ne'.$$

This determines the effect of any homomorphism of rings on all natural multiples of the unity e of S. Every element of the ring Z of integers is a multiple of 1. Thus, given a ring R, the only possible homomorphism $u:Z \longrightarrow R$ is defined by $un = n1'$.

This mapping is a homomorphism. For, in addition to $u1 = 1'$,

$$\begin{aligned} u(n+m) &= (n+m)1' \\ &= (1'+1'+1'+---+1')_{n+m \text{ terms}} \\ &= (1'+1'+---+1')_{n \text{ terms}}+(1'+1'+---+1')_{m \text{ terms}} \\ &= n1'+m1' \\ &= un+um \end{aligned}$$

by the associative property of addition in R and the meaning of natural multiple. Similarly,

$$\begin{aligned} u(nm) &= (nm)1' \\ &= (1'+1'+1'+\text{---}+1')_{nm \text{ terms}} \\ &= (1'+1'+\text{---}+1')_{n \text{ terms}}(1'+1'+\text{---}+1')_{m \text{ terms}} \\ &= (n1')(m1') \\ &= (un)(um). \end{aligned}$$

This completes the proof.[2, pp. 120, 121]

The homomorphism in the previous theorem, defined by $un = n1'$, depends essentially upon the unity elements, so will be called the unital homomorphism for the ring R.

Definition 1.8. An arbitrary ring R has (positive) characteristic n if n is the least positive integer such that $nr = 0_R$ for every r in R. If no such positive integer exists, then R is said to have characteristic zero. If R has unity e, then, for any r in R,

$$nr = n(er) = (ne)r = 0_R,$$

and it follows that the characteristic of R can be defined as the (additive) order of its unity e. Thus, a non-trivial ring R with unity e has a positive characteristic n if n is the least positive integer with $ne = 0_R$ and has characteristic zero if no such multiple ne is 0_R.

Theorem 1.9. Let R be a ring with unity e. If the characteristic of R is a positive integer n, then the image Z' of the unital homomorphism is isomorphic to Z/(n), while if the characteristic of R is zero, then Z' is isomorphic to Z.

Proof. If R has characteristic n, the kernel of the unital homomorphism is (n), and, by Theorem 1.4,

$$Z' \cong Z/(n).$$

If R has characteristic zero, the kernel of the unital homomorphism is (0),

$$Z' \cong Z/(0) = Z,$$

and the theorem is established. [1, p. 139]

Theorem 1.10. Any two nonzero elements b and d in the ring Z of integers have a greatest common divisor (b,d). It can be expressed as a "linear combination" of b and d, with integral coefficients s and t, in the form

$$(b,d) = sb+td.$$ [3, p. 17]

Theorem 1.11. For each prime number p, Z/(p) is a field.

Proof. Z/(p) is a commutative ring with unity 1+(p). Consider any nonzero element a+(p) in Z/(p). Since a+(p) is not equal to zero and p is a prime, (a,p) = 1, and there exist integers s and t in Z such that sa+tp = 1. The unital homomorphism applied to this equation carries prime p to zero, hence s to an inverse s+(p) of a+(p), as required to prove Z/(p) is a field. [2, pp. 157, 158]

CHAPTER II

RINGS CONTAINING FIELDS

I. RINGS WITH POSITIVE CHARACTERISTIC

Now it will be shown that if a ring with unity has positive characteristic $n = pm$, where p is a positive prime and $(p,m) = 1$, then R contains a field isomorphic to the field $Z/(p)$. Before this can be done, it is necessary to introduce some of the properties of a direct sum of rings.

Definition 2.1. Let S_1 and S_2 be any two rings, and consider the set S of all symbols (s_1,s_2) with s_1 in S_1, s_2 in S_2. Defining addition and multiplication by

$$(s_1,s_2)+(t_1,t_2) = (s_1+t_1,s_2+t_2)$$

and

$$(s_1,s_2)(t_1,t_2) = (s_1t_1,s_2t_2),$$

it is easy to verify that the set S, denoted by S_1+S_2, satisfies the minimal requirements for a ring. S is called the direct sum of S_1 and S_2.[4, p. 114]

The zero element of $S = S_1+S_2$ is $(0_1,0_2)$, the first zero being the zero of S_1, the second the zero of S_2. If S_1 and S_2 have unity elements e_1 and e_2 respectively, then S has the unity element (e_1,e_2). If both S_1 and S_2 have more than one element, S has proper divisors of zero since

$$(s_1,0_2)(0_1,s_2) = (0_1,0_2)$$

for every s_1 in S_1, s_2 in S_2. S is a commutative ring if and only if both S_1 and S_2 are commutative. The one-to-one correspondence

$$(s_1,s_2) \longleftrightarrow (s_2,s_1)$$

between elements of S_1+S_2 and S_2+S_1 is an isomorphism, so no distinction is made between the two rings.

The set of all elements of S of the form $(s_1,0_2)$, where s_1 is in S_1, is an ideal S_1' of S isomorphic to S_1 by the correspondence

$$s_1 \longleftrightarrow (s_1,0_2).$$

Similarly, the set of all elements of S of the form $(0_1,s_2)$, where s_2 is in S_2, is an ideal S_2' of S isomorphic to S_2.

If $s = (s_1,s_2)$ is any element of S, the correspondence

$$s \longrightarrow (s_1,0_2)$$

is a homomorphism of S onto S_1'. The elements of S that correspond to the zero element of S_1' are precisely the elements of S_2'. It follows, from Theorem 1.4, that

$$S/S_2' \cong S_1' \cong S_1,$$

and, similarly,

$$S/S_1' \cong S_2' \cong S_2.$$

Since

$$(s_1,s_2) = (s_1,0_2)+(0_1,s_2),$$

it is clear that every element of S is uniquely expressible as a sum of elements of S_1' and S_2' respectively.

Theorem 2.2. If a ring S has positive characteristic $n = n_1n_2$, where n_1 and n_2 are greater than one and $(n_1,n_2) = 1$, then $S \cong S_2+S_1$, where S_i is a ring of characteristic n_i $(i = 1, 2)$.

Proof. Since $(n_1,n_2) = 1$, there exist integers k and h such that

$$1 = n_1k+n_2h,$$

and, hence,

$$s = n_1ks+n_2hs \tag{1}$$

for every s in S. Let S_2 be the set of all elements of S of the form n_1ks, s in S. It follows easily that S_2 is a ring (with unity if S has unity), and its characteristic does not exceed n_2 since

$$n_2(n_1ks) = nks = 0_S.$$

In like manner, the set S_1 of all elements of S of the form n_2hs is a ring (with unity if S has unity) whose characteristic does not exceed n_1.

From (1),

$$n_1ks = (n_1k)^2s+nkhs,$$

and, since $ns = 0_S$, this implies that

$$(n_1k)^2s = n_1ks$$

for every element s of S. Similarly,

$$(n_2h)^2s = n_2hs.$$

These relations will be used presently.

Now the correspondence

$$(2) \qquad s \longleftrightarrow (n_1ks, n_2hs)$$

will be shown to be an isomorphism of S with the direct sum S_2+S_1. If s and t are arbitrary elements of S, then

$$s+t \longrightarrow \big(n_1k(s+t), n_2h(s+t)\big) = (n_1ks, n_2hs)+(n_1kt, n_2ht),$$

and the above relations show that

$$st \longrightarrow (n_1kst, n_2hst) = \big((n_1k)^2st, (n_2h)^2st\big)$$
$$= (n_1ks, n_2hs)(n_1kt, n_2ht).$$

Futhermore,

$$n_1ks+n_2ht \longrightarrow (n_1ks, n_2ht),$$

so that every element of S_2+S_1 is the image of some element of S. It follows that the correspondence (2) is a homomorphism of S onto S_2+S_1. However, if

$$s \longrightarrow (0_2, 0_1),$$

then

$$n_1ks = n_2hs = 0_{S_2S_1S},$$

and (1) shows that $s = 0_{S_2S_1S}$. Thus, the homomorphism has zero kernel and is actually an isomorphism.

To complete the proof of the theorem, it must be shown that the characteristic of S_i is n_i $(i = 1, 2)$. If S_i has characteristic m_i, it has already been pointed out that $m_i \leqq n_i$. If (s_2, s_1) is any element of S_2+S_1, it follows that

$$m_1m_2(s_2, s_1) = (m_1m_2s_2, m_1m_2s_1) = (0_2, 0_1),$$

and the characteristic of S_2+S_1 cannot be greater than

m_1m_2. Since n is the characteristic of S, it is also the characteristic of the isomorphic ring S_2+S_1, and, therefore,

$$n \leq m_1m_2.$$

But $m_i \leq n_i$ implies that

$$m_1m_2 \leq n_1n_2 = n,$$

and

$$n = n_1n_2 = m_1m_2.$$

The fact that $m_i \leq n_i$ $(i = 1, 2)$ also implies that

$$m_i = n_i,$$

and the proof is completed.[4, pp. 116, 117, 118]

By this theorem, whenever a ring R with unity has positive characteristic $n = pm$, where p is a positive prime and $(p,m) = 1$, R contains rings (ideals) R_1 and R_2 with characteristics p and m respectively. By Theorem 1.9, R_1 contains a ring Z' isomorphic to Z/(p), and since Z/(p) is a field as a result of Theorem 1.11, Z' is a field. If e is the unity of R, correspondence (2) from the previous theorem shows that (pke,mhe) must be the unity of the direct sum R_2+R_1, and mhe must be the unity of R_1. Remember h and k must be such that

$$1 = pk+mh.$$

As an example, consider the ring Z/(60) of integers modulo 60 with positive characteristic 60 and unity 1_{60}.

Since $60 = (3)(20)$, $(3,20) = 1$, and

$$\begin{aligned} 1 &= pk+mh \\ &= 3k+20h \\ &= 3(-13)+20(2), \end{aligned}$$

$Z/(60)$ contains a field F_1 with characteristic 3 and unity

$$mhe = (20)(2)(1_{60}) = (40)(1_{60}) = 40_{60}.$$

Similarly, since $60 = (5)(12)$, $(5,12) = 1$, and

$$\begin{aligned} 1 &= pk+mh \\ &= 5k+12h \\ &= 5(-7)+12(3), \end{aligned}$$

$Z/(60)$ contains a field F_2 with characteristic 5 and unity

$$mhe = (12)(3)(1_{60}) = (36)(1_{60}) = 36_{60}.$$

The smallest fields F_1' and F_2' contained in F_1 and F_2 are the additive subgroups generated by the unity elements 40_{60} and 36_{60} respectively. The field F_1' isomorphic to $Z/(3)$ is

$$\left\{40_{60},\ 20_{60},\ 0_{60}\right\},$$

and the field F_2' isomorphic to $Z/(5)$ is

$$\left\{36_{60},\ 12_{60},\ 48_{60},\ 24_{60},\ 0_{60}\right\}.$$

A ring R with unity that has a positive characteristic and no divisors of zero must have a prime characteristic. For suppose the characteristic of R is a composite number $n = kf$, where k and f are two positive integers. If e is the unity of R,

$$ne = (kf)e = (ke)(fe) = 0_R$$

implies that the elements ke and fe are divisors of zero in R. Similarly, any nontrivial ring S contained in R with no divisors of zero must have prime characteristic p less than n.

Suppose a nontrivial ring S contained in R has a prime characteristic p less than n such that $(p,n) = 1$. Then, there exist integers s and t such that

$$1 = ps+nt,$$

and, for all a in S,

$$a = psa+nta = 0_{SR}.$$

This means that if R contains the ring S with prime characteristic p less than n, p must be a factor of n.

Now suppose the characteristic of R is $n = p^k q$, where k is an integer greater than one and $(p,q) = 1$, and suppose R does contain a nontrivial ring S with prime characteristic p. From Theorem 2.2, R is isomorphic to the direct sum of two rings (ideals) R' and R'' contained in R with characteristics p^k and q respectively. Thus, the direct sum R'+R'' must contain a ring S'' isomorphic to S. Since $(p,q) = 1$, there is no nonzero element r'' in R'' such that $pr'' = 0_{R''}$, so the elements of S'' must be from the set R_1' of elements of the form $(r',0_{R''})$ with r' in R' and $0_{R''}$ in R''. Next, the isomorphism

$$r' \longleftrightarrow (r',0_{R''})$$

between R' and R_1' implies that R' must contain a ring S' such that

$$S \cong S'' \cong S'.$$

Remembering that e is the unity of R and $p^{k-1}e \neq 0_R$,

$$p(p^{k-1}e) = p^k e = 0_{R'R}$$

implies that $p^{k-1}e$ must be an element of S' in R'. However,

$$(p^{k-1}e)^2 = p^{2k-2}e^2 = p^{2k-2}e = p^k(p^{k-2}e) = 0_{S'R'R}$$

shows that $p^{k-1}e$ is a divisor of zero in S', and, thus, its corresponding element a in S is a divisor of zero in S.

Therefore, if the characteristic of a ring R with unity is $n = p^k q$, where k is an integer greater than one and $(p,q) = 1$, R cannot contain a ring S of prime characteristic p, so R cannot contain a field. The ring R will contain a field if and only if it has a prime characteristic, or, when expressed as a product of prime factors using exponents, the characteristic contains first degree prime factors. For each of these first degree prime factors p, there is contained in R a field F with characteristic p, and the smallest field contained in F is isomorphic to $Z/(p)$.

II. RINGS WITH ZERO CHARACTERISTIC

In this section, it will be shown that the smallest field contained in a ring with unity, zero characteristic, and no divisors of zero must be isomorphic to the field of rational numbers.

Definition 2.3. If w' is an isomorphism $w':R' \leftrightarrow S'$ of rings R' and S' contained in rings R and S respectively, then an isomorphism $w:R \leftrightarrow S$ will be called an extension of w' if $wr' = w'r'$ for all r' in R'.[1, p. 97]

Definition 2.4. If D is a nonzero integral domain contained in a field F, then

$$K = \left\{ab^{-1} \middle| a, b \text{ in } D, b \neq 0_D\right\}$$

is the quotient field of D in F.[1, p. 99]

Theorem 2.5. Let D and D' be isomorphic integral domains with isomorphism $w:D \leftrightarrow D'$, contained, respectively, in fields F and F', and let K, K' be the respective quotient fields. Then w can be extended in one and only one way to an isomorphism $w':K \leftrightarrow K'$.

Proof. If an extension w' of w exists, then, for ab^{-1} in K, it must be true that

$$w'(ab^{-1}) = (w'a)(w'b^{-1}) = (w'a)(w'b)^{-1} = (wa)(wb)^{-1}.$$

Thus, w' is unique if it exists.

Define $w':K \leftrightarrow K'$ by

$$w'(ab^{-1}) = (wa)(wb)^{-1}$$

for arbitrary ab^{-1} in K. Now

$$\begin{aligned} w'(ab^{-1}) = w'(cd^{-1}) &\text{ iff } (wa)(wb)^{-1} = (wc)(wd)^{-1} \\ &\text{ iff } (wa)(wd) = (wc)(wb) \\ &\text{ iff } w(ad) = w(cb) \\ &\text{ iff } ad = cb \end{aligned}$$

if and only if

$$ab^{-1} = cd^{-1}.$$

Thus, w' is one-to-one.

If xy^{-1} is any element of K', then x, y in D' and $x = wa$, $y = wb$ for some a, b in D, hence, $w'(ab^{-1}) = xy^{-1}$, and w' is onto.

Finally,

$$\begin{aligned} w'(ab^{-1}+cd^{-1}) &= w'[(ad+bc)(bd)^{-1}] \\ &= [w(ad+bc)][w(bd)]^{-1} \\ &= [(wa)(wd)+(wb)(wc)][(wb)^{-1}(wd)^{-1}] \\ &= (wa)(wb)^{-1}+(wc)(wd)^{-1} \\ &= w'(ab^{-1})+w'(cd^{-1}), \end{aligned}$$

and

$$\begin{aligned} w'[(ab^{-1})(cd^{-1})] &= w'[(ac)(bd)^{-1}] \\ &= [w(ac)][w(bd)]^{-1} \\ &= (wa)(wc)(wb)^{-1}(wd)^{-1} \\ &= [(wa)(wb)^{-1}][(wc)(wd)^{-1}] \\ &= [w'(ab^{-1})][w'(cd^{-1})]. \end{aligned}$$

Thus, w' preserves both sums and products and is, indeed, an isomorphism. Since w' trivially agrees with w on elements of D, the theorem is proved.$_{[1,\ pp.\ 99,\ 100]}$

Results of this theorem are needed in the proof of the following theorem.

Theorem 2.6. Let R be a ring with unity e and no divisors of zero. If R has characteristic zero and contains a field F, the smallest field contained in F is isomorphic to the field Q of rational numbers.

Proof. The characteristic of R is zero, so, by Theorem 1.9, the image Z' of the unital homomorphism $u:Z \longrightarrow R$ must be isomorphic to the integral domain Z.

Since R has no divisors of zero, for any nonzero r in R, er = fr implies that $(e-f)r = 0_R$, and e = f. Thus, any field F contained in R must contain Z' isomorphic to Z.

Theorem 2.5 proves that the smallest field containing Z is its quotient field Q. Also, by Theorem 2.5, the smallest field in R containing Z' must be a set Q' isomorphic to Q, and the theorem is established.

As a result of these last two theorems, a ring of zero characteristic and no divisors of zero that contains a field must be an extension of a set isomorphic to the set of rational numbers. This includes any integral domain or division ring with zero characteristic that contains a field. Note that finite integral domains and finite division rings have positive characteristics and are fields.

It is possible for a ring with unity, with zero characteristic, and with divisors of zero to contain a finite field and not contain a set isomorphic to the field of rational numbers. Consider the ring R formed by the direct sum of the ring Z of integers with the field Z/(3) of integers modulo 3. The ring R has divisors of zero.

The unity and zero of R are (1,1') and (0,0'), and there is no positive integer n such that n(1,1') = (0,0'). It is easy to verify that the subset

$$\left\{(0,a) \middle| 0 \text{ in } Z,\ a \text{ in } Z/(3)\right\} = \left\{(0,0'),\ (0,1'),\ (0,2')\right\}$$

is a field isomorphic to Z/(3).

The ring formed by the direct sum of the field Q of rational numbers with the field Z/(3) of integers modulo 3 is an example of a ring with zero characteristic and divisors of zero that contains a subset isomorphic to Q and another subset isomorphic to Z/(3).

The direct sum Q+Q of the field Q of rational numbers with itself is a ring with unity, zero characteristic, and divisors of zero that contains an infinite field but no finite field.

CHAPTER III

MULTIPLICATIVE INVERSES

Again consider the ring R with unity element e and positive characteristic n = pm, where p is a positive prime and (p,m) = 1. It has been shown that R contains a ring (ideal) R' with characteristic p. It has also been shown that R' contains a field F, and the unity e' of R' is also the unity of F. Every nonzero element b in F must have a multiplicative inverse b^{-1} in F. Does b in F have a multiplicative inverse in R? Does b in F have a multiplicative inverse in R' other than b^{-1}? These questions will be answered in the remainder of this chapter.

In the ring R, a nonzero element that has a multiplicative inverse cannot be a proper divisor of zero in R. For if c and d are nonzero elements of R, (c)(d) = 0_R, and c^{-1} exists, then

$$(c^{-1})(c)(d) = (c^{-1})(0_R),$$

and d = 0_R. Similarly, if d^{-1} exists, then c = 0_R.

Now let b be an arbitrary nonzero element of the field F contained in R, and suppose there exists an element r in R such that (b)(r) = e (the unity of R). The element b in F is also an element of the ideal R', and by the definition of an ideal, if such an r existed, R' would contain e and the entire ring R. Therefore, the nonzero elements of F, as well as all the other nonzero elements of the ideal R', have no multiplicative inverses in the ring R. They are proper divisors of zero in R.

Next, suppose there exists an element $y \neq b^{-1}$ in R' such that $(b)(y) = e'$ (the unity of R'). Then $(b)(b^{-1}) = (b)(y)$. However, since b^{-1} in R' exists, b is not a proper divisor of zero in R', and $b^{-1} = y$.

Thus, a nonzero element b in F has a unique multiplicative inverse relative to R, R', and F. That being the element b^{-1} in F such that $(b)(b^{-1}) = e'$ (the unity of F).

CHAPTER IV

SUMMARY AND CONCLUSIONS

I. RINGS WITH POSITIVE CHARACTERISTIC

A ring R with unity e and positive characteristic n contains a field F if and only if n = pm and (p,m) = 1, where p is a positive prime. The characteristic of F is p, and the elements of F are divisors of zero in R.

If the integers k and h are such that

$$1 = pk+mh,$$

then the unity of F is

$$e' = mhe,$$

and the smallest field F' contained in F is the additive subgroup generated by e'. F' is isomorphic to the field Z/(p) of integers modulo p.

Express the characteristic of R as a product of prime factors using exponents. For each first degree prime factor p, there is contained in R a field F with characteristic p.

II. RINGS WITH ZERO CHARACTERISTIC

Any ring R with unity e, zero characteristic, and no divisors of zero that contains a field must be some extension of a field isomorphic to the field of rational numbers.

If a ring R with unity e and zero characteristic has divisors of zero, no conclusions have been reached as to when R might or might not contain a field. If R contains a field at all, it may contain a finite field, an infinite field, or both.

BIBLIOGRAPHY

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

2. Birkhoff, Garrett and Saunders MacLane. *Algebra*. New York: The Macmillan Company, 1968.

3. Birkhoff, Garrett and Saunders MacLane. *A Survey of Modern Algebra*. Third edition. New York: The Macmillan Company, 1965.

4. McCoy, N. H. *Rings and Ideals*. Buffalo: The Mathematical Association of America; LaSalle, Illinois: The Open Court Publishing Company, 1948.

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

6. Miller, K. S. *Elements of Modern Abstract Algebra*. New York: Harper & Brothers, 1958.