AN INVESTIGATION OF INFINITE FIELDS
OF NON-ZERO CHARACTERISTIC

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teachers College

In Partial Fulfillment

of the Requirements for the Dogree

Master of Arts

by

Melvin R. Roy

August, 1968

Approved for the Major Department

Marion P. Emerson

Approved for the Graduate Council

Laurence C. Boylan

ACKNOWLEDGEMENTS

This writer would like to thank Dr. Marion P. Emerson for his guidance and assistance in the development of this paper.

Also, I am greatly indebted to my wife, Joyce, for her patience and assistance.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

In the study of algebraic disciplines, one encounters a number of properties which classify and compare various mathematical structures. The appearance of many systems would tend to set them apart from others, however, upon careful examination, we find that the basic systems in reference are indeed quite similar. The property which will be discussed in this thesis is the characteristic of a field, and in particular, the infinite fields of non-zero characteristic.

In order to define "characteristic", as it is to be used in this thesis, requires a review of a number of concepts from the theory of rings. However, the reader is assumed to have knowledge of the basic concepts of the theory of groups, rings, and fields.

Rings. Example 1.1. The set of integers, I, is a ring. The verification of this fact can be demonstrated by verifying that the ring properties hold in I. This verification is not essential to the development of this thesis. The importance of this example is to point out that under certain conditions, a subset of a ring is again a ring. Consider the subset of I which are integral multiples of two. This set also by definition is a ring. This gives an illustration of the subring which is the basic reason for the example. With this idea of subring in mind, consider the example of all integral multiples of two as a subring of I. Not only are the integral multiples of two closed with respect to multiplication, but the product of any $a \in I$ and any integral multiple of two, gives an integral multiple of two.

That is: $\forall\, a \in I$ and $\forall\, b \in \{$integral multiples of two = $2B$, $B \in I\}$ $(2B)a = a(2B) = 2(aB)$.

When this condition exists, the subring is an ideal.

Definition 1.2. If N is a subring of a ring R such that both ra and ar are elements in N for all elements a of N and all ring elements r in R, then N is an ideal, (sometimes called a two-sided ideal).

Consider two rings $\langle R, +, \cdot\rangle$ and $\langle R', \oplus, x\rangle$. If a mapping ϕ exists so that $\phi(a + b) = \phi(a) \oplus \phi(b)$ and $\phi(a \cdot b) = \phi(a) \times \phi(b)$, for all a and b in R then ϕ is a homomorphism. Suppose further that ϕ is a one to one mapping of R onto R'. Then ϕ is an isomorphism, written $R \approx R'$.

Theorem 1.1. Let ϕ be a homomorphism mapping the ring R onto R'. Then the set of elements N of the preimages of the additive identity 0' of R' forms an ideal in R.

[7, p. 74]

Returning now to the example of an ideal, namely the set of integral multiples of two in the ring of integers I, a set of elements of the form (a + n) can be obtained where "a" is a fixed element of I and n ranges throughout the set of even integers. Then a + n for any specific "a" is a remainder class or residue class. This set of remainder classes are referred to as $^R/_N$ where N is the ideal of even integers in R.

Theorem 1.2. Let Φ be a homomorphism mapping R onto R'. Let N be the set of elements in R which map onto the idenity 0' in R'. Then N is an ideal in R and the remainder classes $^R/_N$ is a ring isomorphic to R'. [7, p. 76]

Definition 1.3. Let R be a ring and let M be an arbitrary subset of R. The intersection of all ideals containing this set M is called the ideal generated by M and is written (M).

If M consists of a single element "a", then the ideal is written (a). An ideal such as (a) generated by a single element is called a principal ideal. [7, p. 78]

Definition 1.4. Let R be a ring and N an ideal in R. If N has the property that whenever $a \cdot b \in N$ then either a or b is in N; then N is called a prime ideal. [7, p. 79]

For example, the principal ideal (7) is prime in the ring of integers I, since if $a \cdot b$ is in (7), a or b must be a multiple of 7. On the other hand (6) is not a prime ideal as $12 = 3 \cdot 4$ is in (6) but neither 3 nor 4 is in (6).

Fields. Consider the remainder classes $^I/_{(7)}$. This partitions the set I into classes, 0 + 7n, 1 + 7n, 2 + 7n, 3 + 7n, 4 + 7n, 5 + 7n, 6 + 7n where $n \in I$. Let 0, 1, 2, 3, 4, 5, 6, represent each of these classes respectively. It can be shown that this set forms a field.

The familiar number systems of analysis, the rational complex numbers are examples of

s. These fields are infinite fields as each contains an infinite set of elements. The example $^{I}/_{(7)}$ is an example of a field containing a finite number of elements. If p is a prime number, then $^{I}/_{(p)}$ (the ring of integers mod p) is a field. [3, p. 91]

Consider then, an arbitrary field F. It may be that F contains a subset p which is also a field. If it does, p is referred to as a subfield of F. It is possible that the subfield p also contains a subfield p' and $p' \supset p''$, p'' also a subfield. As the intersection of any number of subfields is again a subfield, the field which is obtained by this intersection of subfields is called the prime field of F.

Definition 1.5. The field obtained by the intersection of all subfields of a field F, is said to be the prime field of F. The symbol π will be used to designate the prime field of F.

Definition 1.5 gives rise to two important facts: (1) every field has a prime field and (2) this prime field is unique.

Theorem 1.3. A field F contains one and only one prime field π.

Proof. Suppose F contains no proper subfields. The field F is then the prime field of F. If F contains subfields U_1, U_2, U_3, . . . U_n, then each of the U_i's must contain the zero element of F. As each U_i is a field, each U_i must contain an identity e_i such that $e_i \cdot U_i = U_i$. However, if e_f is the identity element of F, $e_f \cdot e_i = e_i$. As e_i is the identity of U_i, $e_i \cdot e_i = e_i$. Therefore, $e_f \cdot e_i = e_i \cdot e_i$ and by the cancelation law, $e_f = e_i$. This demonstrates that each U_i must contain "0" and "1" of the field F. If "a" is a non-zero element of each U_i then a^{-1} and -a must also be in each U_i. Therefore, the intersection of all subfields of F is a field. Thus the existance of π is established. Suppose that some field F contains two distinct prime fields π_1, and π_2. This would imply that there exists an element "a" in π_2 such that "a" is not an element of π_1. However, "a", an element of π_2, implies that "a" is an element of every subfield of F. If "a" is an element of every subfield of F, "a" is an element of π_1 by definition of "prime field". Therefore, $\pi_1 = \pi_2$ and the prime field π of F is unique.

The investigation of a prime field yields the remarkable result that every prime field is either isomorphic to the field of rational numbers or else is isomorphic to the ring of residue classes $^I/_{(p)}$ where p is a prime number.

Lemma. Let π be a prime field and e the unity element of π. Then the integral multiples of e form a commutative ring P with unity element.

Proof. By the meaning of "unity element", $n \cdot e = n$ and $m \cdot e = m$. Therefore, $n \cdot e + m \cdot e = n + m$ which is equal to $(n + m)$ e. Also, $(n \cdot e) \cdot (m \cdot e) = n \cdot m = (n \cdot m)$ e. Hence, P is closed with respect to addition and multiplication.

$0 \cdot e = 0$ and $1 \cdot e = e$ are elements of P and if $n \cdot e \in P$, $-n \cdot e$ is also an element of P and $n \cdot e + (-n \cdot e) = 0$. Commutativity and associativity of both operations and the distributive law follow these properties in I.

Theorem 1.4. Let π be a prime field. Let I be the ring of integers and K the field of rational numbers. Then π is a field which is either isomorphic to K or isomorphic to the ring of remainder classes $^{I}/_{(p)}$ where p is a prime number.

Proof. Let p be the ring of integral multiples of e defined in the lemma. Define a mapping f of I onto p by,

$$f : m \longrightarrow me.$$

By definition of addition and multiplication of elements in p, f is a homomorphism. Let N be the ideal in I which maps onto the zero element of p under this homomorphism. By theorem 1.2, $^{I}/_{N}$ is isomorphic to p. Since p is a subset of a field, it can have no divisors of zero. Since $^{I}/_{N}$ is commutative ring with unity element, it is an integral domain and N is a prime ideal. [7, p. 82]

That is:

N = (p) where p is a prime number or zero. Three cases arise.

Case 1. P is a prime number and (p) is a non-trivial prime ideal. That is, (p) is unequal to the null ideal or the unit ideal.

Case 2. $P = 0$ and (p) is the null ideal.

Case 3. $P = 1$ and (p) is the unit ideal.

Case 1. Suppose p is a prime number. Then

$$I/_{(p)} \approx p.$$

Since $I/_{(p)}$ is a field and p is a subset of π, $p = \pi$. This follows from the fact that π is a prime field and does not contain a field as a proper subset. $\therefore$ $I/_{(p)} \approx \pi$

Case 2. Suppose $p = 0$. Then the homomorphism

$$f : I \longrightarrow p$$

becomes an isomorphism,

$$I \approx p$$

since $I/(p) = I/_{(0)} = I$.

Now p is not a field as the ring of integers I is not a field. Since p is a subset of π and π is a field, π must contain all elements of I and the multiplicative inverse of each. That is, π must contain the quotient field A of I. As the quotient field of I is the set of rational numbers Ra, π then must contain Ra. But π is a prime field and therefore contains no field as a proper subset and we conclude $\pi \approx$ Ra.

Case 3. Suppose $p = 1$. Then (1) is the unit idea and $I/(1)$ contains only the element zero. Since

$$I/(1) \approx p$$

this implies p contains only the element 0. This is a contradiction as p must contain 0 and 1. This rules out the case of $p = 1$. [7, pp. 126, 127]

Characteristic. Definition 1.6. If "p" from theorem 1.4 is a prime number, then $I/(p)$ is a finite field. The number p is called the characteristic of the prime field Π and of the original field F. If Π has an infinite number of elements then Π or F is a field of characteristic zero.

It is obvious that if a field is of characteristic zero, it must have an infinite number of elements as the prime field Π of F already would have an infinite number of elements. However, the converse of this statement is not true. That is, a field can have an infinite number of elements with characteristic $p \neq 0$.

CHAPTER II

DEVELOPMENT OF THE INFINITE FIELDS OF NON-ZERO CHARACTERISTIC

It has been established in chapter I that a field of characteristic zero must contain an infinite number of elements. The existance of an infinite set of elements in a field, however, does not imply that the characteristic of this field is zero.

Example 2.1. Consider the field $F = {}^{I}/_{(3)}$. Let $\{0,1,2\}$ represent the remainder classes of ${}^{I}/_{(3)}$. Consider now the polynomials in "x" over F. One element of this ring is the polynomial $x^2 - 2$. As an equation in standard form, this polynomial gives rise to the equation, $x^2 - 2 = 0$. This equation implies that $x \cdot x = 2$ or by conventional notation, $x = \sqrt{2}$. The fact that the square root of two is not an element of F is established by the following lemma.

Lemma: The solution "x" of $x^2 = a$, "a" being a non-zero element of ${}^{I}/_{(p)}$, with $p \neq 2$ is an element of ${}^{I}/_{(p)}$ only if "a" is not a generator of the cyclic multiplicative group of non-zero elements of ${}^{I}/_{(p)}$.

Proof. Suppose the solution of $x^2 = a$ is an element of ${}^{I}/_{(p)}$ and "a" is a generator of the multiplicative group of ${}^{I}/_{(p)}$. If "a" is a generator then $a^n = x$ for some $n \in I$, $n \leq p$. By assumption, $x^2 = a$, and by substitution $(a^n)^2 = a$

which implies $a^{2n} = a$. However, by the "Theorem of Fermat", [2, p. 25], if P is prime and a is not a multiple of p, then $a^{p-1} = 1 \bmod p$. This implies $a^p = a$. Therefore, $a^p = a^{2n}$, but p is prime which means n must be equal to p. However, $n = p$ leads to $a^2 = a$ which implies $a = 0$ or $a = 1$ neither of which can be a generator of the multiplicative group of $^I/_{(p)}$. As the element two is a generator of the multiplicative group of $^I/_{(3)}$, $x^2 = 2$ has no solution in $^I/_{(3)}$.

Suppose that it is desired that the field F be extended so as to contain the solution ($\sqrt{2}$) of the equation $x^2 - 2 = 0$. It is observed that under the operation of multiplication, the set F becomes $\{0,1,2,\sqrt{2},2\sqrt{2}\}$. Upon inspection of this set, multiplication is closed; that is $\sqrt{2} \cdot 2\sqrt{2} = 2\sqrt{2}\sqrt{2} = 2 \cdot 2 = 1$ in (F extended). This set of elements, excluding zero, is a commutative group under the operation of multiplication; however, addition is not closed as $1 + \sqrt{2}$, $1 + 2\sqrt{2}$, $2 + \sqrt{2}$ and $2 + 2\sqrt{2}$ are not elements of F extended. The addition of these elements to the set $\{0, 1, 2, \sqrt{2}, 2\sqrt{2}\}$ gives $\{0, 1, 2, \sqrt{2}, 2\sqrt{2}, 1 + \sqrt{2}, 1 + 2\sqrt{2}, 2 + \sqrt{2}, 2 + 2\sqrt{2}\}$. This set consists of all elements of the form $a + b\sqrt{2}$ where $a, b \in {}^I/_{(3)}$. It can be shown that this set of nine elements is a field.

The notation $F(\sqrt{2})$ will be used to represent the extension field, F extended by $\sqrt{2}$. The polynomial function, $x^2 - 2 = 0$, is called the defining equation of the extension. A field of nine elements has thus been developed which has as its prime field the original field $F = {}^I/_{(3)}$. This would indicate that the characteristic of $F(\sqrt{2})$ is three. As $\sqrt{2}$ is algebraic over the ring of polynomials in x over F, the extension field $F(\sqrt{2})$ is said to be obtained by an algebraic extension of F. In particular, a simple algebraic extension has been made since only one element has been adjoined to $I/(3)$.

The preceding example of a field extension indicates that if a finite field could be extended to an infinite field, this infinite field would have as its prime field the original finite field and would be an infinite field of non-zero characteristic.

Example 2.2. Let F(x) represent the set of all rational functions in "x" of the form:

$$\frac{a_0 + a_1 x + a_2 x^2 + \cdot \cdot \cdot + a_n x^n}{b_0 + b_1 x + b_2 x^2 + \cdot \cdot \cdot + b_m x^m}$$

Where: $a_i,\ b_j \in I/(3)$ and $b_0 + b_1 x + b_2 x^2 + \cdot \cdot \cdot + b_m x^m \neq 0$.

The one to one correspondence:

$$\frac{a_0 + a_1 x + a_2 x^2 + \cdot \cdot \cdot + a_n x^n}{b_0 + b_1 x + b_2 x^2 + \cdot \cdot \cdot + b_m x^m} \leftrightarrow \frac{a_0 + a_1 x^2 + a_2 x^4 + \cdot \cdot \cdot + a_n x^{2n}}{b_0 + b_1 x^2 + b_2 x^4 + \cdot \cdot \cdot + b_m x^{2m}}$$

where, $$\sum a_n x^n \longrightarrow \sum a_n x^{2n}$$

is an illustration of a one to one correspondence from F(x) to a proper subset of F(x). This correspondence demonstrates that F(x) is indeed an infinite set. The field properties can be verified for the operations addition and multiplication. The subset of F(x) consisting of the elements of the form $\frac{a_0}{b_0}$, where a_0 ranges throughout $I/(3)$ and $b_0 = 1$, is $I/(3)$.

Example 2.2 is an infinite field of non-zero characteristic.

Example 2.3. Let $F(\sqrt{2})$ be the finite field of example 2.1. Consider the field extension, $F(\sqrt{2})(\pi)$, where π is transcendental over the extension field, $F(\sqrt{2})$.

$$F(\sqrt{2})(\pi) = \frac{a_0 + a_1\pi + a_2\pi^2 + \cdot\cdot\cdot + a_n\pi^n}{b_0 + b_1\pi + b_2\pi^2 + \cdot\cdot\cdot + b_m\pi^m}$$

Where: a_i, $b_j \in F(\sqrt{2})$.

As in example 2.2 this extension field is an infinite field and the characteristic is non-zero. Although this field extension appears to be the same as the extension field of example 2.2, it is to be observed that the coefficients a_i, b_j are elements of an extension field. The significance of this minor variation will be evident in chapter III.

Example 2.4. Consider the set of 2 x 2 matrices of the form,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

where, a, b $\in {}^{I}/_{(3)}$. This set of matrices consists of the elements:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}.$$

With tho usual definition of multiplication and addition of matrices, the above set of matrices forms a field. The products and sums of the entries a_i, b_j are understood to be as defined in $^I/_{(3)}$. This set of matrices contains the subfield,

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

The field of nine matrices is of characteristic three. If F represents this field of nine matrices, let F(x) represent the set of rational functions in the indeterminate x of the form:

$$\frac{a_0 + a_1 x^1 + a_2 x^2 + \cdot \cdot \cdot + a_n x^n}{b_0 + b_1 x^1 + b_2 x^2 + \cdot \cdot \cdot + b_m x^m},$$

where a_i, $b_j \in F$ and $\sum b_j x^j \neq 0$.

If $\sum_{i=1}^{n} a_i \; x^i = 0,$ $\sum_{j=1}^{m} b_j \; x^i = 0.$

$$b_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and a_0 ranges throughout F, then the set of nine matrices which make up the field F are obtained. The field F being of characteristic three. Thus F(x) is an infinite field of non-zero characteristic.

<u>Examole</u> 2.5. Consider the rational functions in x with coefficients in $^I/_{(3)}$. Call this field F(x). Develop the set of matrices of the form:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

where, a, b $\in$ F(x).

Let M(F(x)) represent this set of matrices.

M(F(x)) =

$$\begin{pmatrix} \dfrac{a_0 + a_1x + \cdot \cdot \cdot + a_nx^n}{b_0 + b_1x + \cdot \cdot \cdot + b_mx^m} & \dfrac{c_0 + c_1x + \cdot \cdot \cdot + c_px^p}{d_0 + d_1x + \cdot \cdot \cdot + d_qx^q} \\ -\dfrac{c_0 + c_1x + \cdot \cdot \cdot + c_px^p}{d_0 + d_1x + \cdot \cdot \cdot + d_qx^q} & \dfrac{a_0 + a_1x + \cdot \cdot \cdot + a_nx^n}{b_0 + b_1x + \cdot \cdot \cdot + b_mx^m} \end{pmatrix}$$

where,

$$\sum b_jx^i \,,\ \sum d_jx^i \neq 0.$$

This set of 2 x 2 matrices is an infinite field. The prime field of M(F(x)) is the set of three matrices:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Therefore, M(F(x)) is an infinite field of characteristic three.

<u>Example</u> 2.6. The infinite field of non-zero characteristic of example 2.2 is a transcendental extension of a finite field. Consider a transcendental extension of the extended field of example 2.2. Let F(x) represent the rational function in x with coefficients in $^{I}/_{(3)}$. Let θ be an element which is transcendental over F(x). Let F(x)(θ) represent all rational functions in θ with coefficients in F(x). That is:

$$F(x) \quad = \quad \frac{\sum a_i \ x^i}{\sum b_j \ x^j}$$

where

$$\sum b_j\, x^j \neq 0,\ a_i,\ b_i \in {}^{I}/_{(3)}$$

and

$$F(x)(-\!\ominus\!-) \quad = \quad \frac{\sum \left(\dfrac{\sum a_i x^i}{\sum b_j x^j} \right) {}_n\!\ominus^{n}}{\sum \left(\dfrac{\sum a_r x^r}{\sum b_s x^s} \right) {}_m\!\ominus^{m}}$$

$$a_i,\ a_r,\ b_j,\ b_s \in {}^{I}/_{(3)}$$

where,

$$b_j x^j \neq 0 \text{ and} \sum \left(\frac{\sum a_r x^r}{\sum b_s x^s} \right) {}_m\!\ominus^{m} \quad \neq \quad 0.$$

As the coefficients of $-\!\ominus\!-$ is an infinite set and $F(x)(-\!\ominus\!-)$ is a field. $F(x)(-\!\ominus\!-)$ is an infinite field. To develop the prime field of $F(x)(-\!\ominus\!-)$, let m, n, i, j, r, s, equal 0. $F(x)(-\!\ominus\!-)$ then becomes:

$$\frac{\sum \dfrac{\sum a_i}{\sum b_j}}{\sum \dfrac{\sum a_r}{\sum b_s}}$$

Let $a_r = b_s = 1$ and $b_j = 1$

and let a_i range throughout ${}^{I}/_{(3)}$.

The above set is $\{o, 1, 2\} \quad = {}^{I}/_{(3)}$. $F(x)(-\!\ominus\!-)$ is an infinite field of characteristic three.

The characteristic of the field in each of the preceding examples is three. The generalization of the forms of infinite fields of non-zero characteristic is not destroyed by this fact. It is obvious that the coefficients of the rational function in (x) as well as the coefficients of the powers of θ in example 2.3 could have been taken from any finite field or any algebraic extension of a finite field.

The examples of this chapter indicate that similarities occur in comparing the various infinite fields of characteristic three. However, upon examination of these examples, many differences become evident. These similarities and differences will be examined from a more general point of view in chapter III.

CHAPTER III

COMPARISONS OF THE VARIOUS FORMS OF INFINITE FIELDS OF NON-ZERO CHARACTERISTIC

When comparing algebraic structures, the existance or absence of isomorphisms is one of the most important and informative relations which can be established. Many conjectures involving isomorphisms are suggested by the examples presented in chapter II. It is these conjectures which will be investigated in this chapter.

Develop the field of rational functions in the indeterminate x as in example 2.2 with coefficients from the field $^{I}/_{(5)}$. Remembering that an isomorphism must be a one to one correspondence which preserves operations, it becomes obvious that no isomorphism exists between example 2.2 and the field described above.

That is:

$$\begin{array}{ccc} \underline{^{I}/_{(3)}(x)} & & \underline{^{I}/_{(5)}(x)} \\ 1 \cdot x & \longleftrightarrow & 1 \cdot x \\ 2 \cdot x & \longleftrightarrow & 2 \cdot x \end{array}$$

$$(1 \cdot x) + (2 \cdot x) = 0 \cdot x = 0 \text{ in } {}^{I}/_{(3)}(x)$$

does not correspond to

$$(1 \cdot x) + (2 \cdot x) = 3 \cdot x \text{ in } {}^{I}/_{(5)}(x).$$

This illustration gives rise to a theorem.

<u>Theorem</u> 3.1. An infinite field F of non-zero

characteristic is isomorphic to a field F' of non-zero characteristic only if the characteristic p of F is equal to the characteristic p' of F'.

Proof. Let ϕ represent an isomorphism from F to F'. Let the prime field π of F = $\{0, 1, 2, \cdots p\}$. Let the prime field π' of F' = $\{0, 1, 2, \cdots p \cdots p'\}$. Suppose that $p \neq p'$. The generality of the proof will not be lost by further assuming $p' > p$. With this assumption and the fact that ϕ is an isomorphism, set up the following correspondence.

$$\begin{array}{rcccl} & 0 & \xleftrightarrow{\phi} & 0 & \\ & 1 & \xleftrightarrow{\phi} & 1 & \\ & 2 & \xleftrightarrow{\phi} & 2 & \\ & \vdots & & \vdots & \\ & p & \xleftrightarrow{\phi} & p & \\ p + 1 = & 0 & \xleftrightarrow{\phi} & p + 1 & \neq p' + 1 \end{array}$$

$$\text{But } p' + 1 = 0.$$

This contradicts the fact that ϕ is an isomorphism. The supposition that $p \neq p'$ led to this contradiction and therefore $p = p'$.

Theorem 3.1 can be used in two ways. It assures that if two fields of non-zero characteristic are isomorphic then they must be of the same characteristic p. Theorem 3.1 also points out that a prerequisite for an isomorphism to exist from one field of non-zero characteristic to another is that they be of the same characteristic.

It may seem that equality of characteristics is sufficient to conclude that two fields of non-zero characteristic are isomorphic. Consider, however, examples 2.2 and 2.3. Here are two fields of characteristic three which obviously are not isomorphic.

In order to investigate the existance of isomorphisms relating the algebraic systems in question, it is helpful to consider generalizations involving only simple extensions of a finite field.

Theorem 3.2. Let F be a field and θ an arbitrary transcendental element in a field containing F. Let x be an indeterminate. Then $F(\theta)$ is a field which is isomorphic to F(x) where F(x) is the set of rational functions in the indeterminate x with coefficients in F.

Proof. Since F and θ are elements of a field, then $F(\theta)$ is a field obtained by the adjunction of θ to F. This field must contain $F[\theta]$ which is the set of polynomials in θ over F. Let $F[x]$ be the ring of polynomials in the indeterminate x over F. $F[\theta]$ is all elements of the form $\sum a_n\theta^n$ where $a_n \in F$. Define a mapping ϕ,

$$\phi : \quad \sum a_n x^n \longrightarrow \sum an\theta^n$$

of $F[x]$ onto $F[\theta]$ where $f(x) = \sum a_n x^n \in F[x]$ and $f(\theta) = \sum a_n\theta^n \in F[\theta]$.

With the usual definition of multiplication and addition of polynomials, ϕ is a homomorphism. The mapping ϕ can also be shown to be an isomorphism. Suppose that ϕ is not an isomorphism. Let N be the kernel of ϕ. If $f(x) \neq 0$ in $F[x]$ is in N, then $f(x) \xrightarrow{\phi} 0$. However, by definition of ϕ, $f(x) \xrightarrow{\phi} f(\theta)$. This implies that $f(\theta) = 0$ which is a contradiction of the assumption that θ is transcendental over F. This establishes ϕ to be an isomorphism:

$$F[x] \longleftrightarrow F[\theta]$$

now $F[\theta]$ is not a field since $F[x]$ is not a field. However, if two integral domains are isomorphic then their quotient fields are isomorphic. Therefore, $F(x)$ is isomorphic to $F(\theta)$.

Theorem 3.2 has a very important implication. It assures that the investigation of rational functions in an indeterminate x over a field F will yield results applicable to all simple transcendental extensions of F.

It becomes apparent that the finite field F from which the coefficients of x^i are taken in F(x), determines the existance or absence of an isomorphic mapping from one infinite field of non-zero characteristic to another. A suitable vehicle to obtain certain properties of F is the vector space.

Example 3.1. Consider the field $F(\sqrt{2})$, $F = {}^{I}/_{(3)}$. The prime field Π of $F(\sqrt{2})$ is the field of remainder classes ${}^{I}/_{(3)}$. As $F(\sqrt{2})$ contains Π, it may be considered as a vector space over Π. The two independent vectors (1, 0) and $(0, \sqrt{2})$ form a basis of this vector space as every element is of the form $a + b\sqrt{2}$, $a, b \in \pi$. The dimension of this vector space is two and is written $(F(\sqrt{2});\pi) = 2$. Notice that $F(\sqrt{2})$ consists of nine elements. The characteristic of the field is three and the dimension of $F(\sqrt{2})$ over π is two. The relation $9 = 3^2$ leads to the following theorem.

Theorem 3.3. Let F be a finite field and π its prime field. Then the number of elements q in the field F is equal to p^n where n is the dimension of F over π and p is the characteristic of F.

Proof. Since $n = (F : \pi)$ is finite, the field F considered as a vector space over π has a finite basis say,

$$v_1, v_2, v_3, \cdots v_n .$$

Every element U of F can be expressed as a linear combination of the v_i's with coefficients in π:

$$U = a_1v_1 + a_2v_2 + \cdots + a_nv_n \; ; a_i \in \pi .$$

Now in any expression,

$$b_1v_1 + b_2v_2 + b_3v_3 + \cdots + b_nv_n \quad b_j \in \pi = I/_{(p)},$$

there are p distinct values which the b_j's may assume, since there are p distinct elements in $\pi = I/(p)$. Hence, there are at most p^n elements in F.

Suppose two of these p^n elements are equal.

$$b_1v_1 + b_2v_2 + \cdots + b_nv_n = c_1v_1 + c_2v_2 + \cdots + c_nv_n$$

where $b_i \neq c_i$ for some b_i, c_i.

Subtracting $c_i v_i$ from both members of the preceding equation yields;

$$(b_1-c_1)\ v_1 + (b_2-c_2)\ v_2 + \cdot\ \cdot\ \cdot + (b_n-c_n)\ v_n = 0$$

where not all $b_i-c_i = 0$. This implies that the v_n's are linearly dependent which contradicts the assumption that they form a basis. Therefore, there are exactly p^n elements in F. [7, p. 159]

Using theorem 3.3 and the fundamental theorem of arithmetic, (the fundamental theorem of arithmetic establishes the uniqueness of p^n for if $p^n = q^m$, p and q both prime, then the number $A = p^n = q^m$ would have two distinct prime factorizations), the characteristic of a finite field of n elements is unique.

These properties of the finite field from which the coefficients of x are taken in F(x) leads to the basic and most powerful theorem with regard to the isomorphisms of the structures under consideration.

Theorem 3.4. Two fields F(x) and F'(x) of non-zero characteristic are isomorphic if and only if the fields F and F' are isomorphic.

Proof. Let F(x) be isomorphic to F'(x). F is a subset of F(x) and F' is a subset of F'(x). If f is the isomorphism from F(x) to F'(x), the same mapping f, will relate F and F' as an isomorphism.

Let F be mapped to F' by g where,

$$g\ :\ F \longleftrightarrow F' \text{ is an isomorphism.}$$

That is:

$$\begin{aligned} g\ (a_1) &= a_1{}' \\ g\ (a_2) &= a_2{}' \\ &\vdots \\ g\ (a_n) &= a_n{}' \\ &\vdots \end{aligned}$$

Now F(x) contains F[x]and F'(x) contains F'[x]. Let F[x] be mapped to F'[x] by g.

$$g \quad : \sum a_i x^i \longrightarrow \sum a_i{}' x^i$$

where,

$$a_i \in F \text{ and } a_i{}' \in F'.$$

By definition of addition and multiplication of polynomials, g is a homomorphism. Suppose g is not an isomorphism. This would imply that;

$$g \ (\sum a_i x^i) = \sum a_i{}' x^i$$

and

$$g \ (\sum a_j x^j) = \sum a_i{}' x^i$$

for some i and j.

However, by definition of g, a_j would then equal a_i, and g is an isomorphism. If F[x] is isomorphic to F'[x] then F(x) is isomorphic to F'(x).

Theorem 3.4 placed no conditions on F and F'. However, previous theorems require that F and F' be of the same characteristic. The fields F and F' may be finite or infinite.

Theorem 3.4 may appear to be the same as theorem 3.3. The difference can best be shown by an example. Theorem 3.3 implies that any simple transcendental extension of a field F, is isomorphic to the rational functions in the indeterminate x with coefficients in the same field F. Theorem 3.4 implies that any two fields which are obtained by a transcendental extension of two fields F and F' are isomorphic if F is isomorphic to F'. Theorem 3.4 also implies that if two fields F and F' are extended by a single transcendental element respectively so that $F(\Theta)$ is isomorphic to $F'(\Theta')$, then F must be isomorphic to F'.

Consider the field $F(\Theta)$ where F is $^{I}/_{(3)}(\sqrt{2})$. This set F consists of the nine elements of the form $a + b\sqrt{2}$, where $a, b \in {}^{I}/_{(3)}$. Also consider the field M(x) where M is the set of 2 x 2 matrices of the form:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

and

$$a, b \in {}^{I}/_{(3)}.$$

The determinants of this set M are equal to the sums, $a^2 + b^2$ where $a, b \in {}^{I}/_{(3)}$.

Define f so that:

$$f \quad : \quad a^2 + b^2 \longrightarrow a + b\sqrt{2}.$$

The mapping f establishes that M is isomorphic to F and by theorem 3.4, M(x) is isomorphic to $F(\theta)$. Example 2.5 could be considered as the field $T(\theta)$ where T = F(x). Thus 3.4 would imply that in order for a field $G(\theta')$ to be isomorphic to $T(\theta)$. G must be isomorphic to F(x). Where F(x) is understood to be $^{I}/_{(p)}$ extended by the indeterminate "x".

CHAPTER IV

CONCLUSION AND SUGGESTIONS FOR FURTHER STUDY

The investigation of an axiomatic structure of an unusual type, amplifies the importance of structure in the study of ordinary algebra. The structures which have been considered in this thesis are fields having the basic properties of the rational, real, and complex number fields. These fields of non-zero characteristic have many differences. The property of being algebraically closed is not one of the properties of fields of non-zero characteristic.

The development of infinite fields of non-zero characteristic involves both the algebraic extensions and the transcendental extensions of finite fields. This gives a better understanding of the importance of the completeness property enjoyed by the complex field.

Certain properties of the structures under investigation in this thesis seem contradictory in nature. However, these properties point out the value of the corresponding properties in the fields of analysis. For example, in a field of characteristic p, $(x + y)^p = x^p + y^p$. The verification of this property follows from the algorithm of the binomial expansion.

$$(x + y)^p = x^p + px^{p-1}y + \frac{p(p-1)}{2!}x^{n-2}y^2 + \cdot \cdot \cdot + y^p$$

It will be observed that the numerator of each numerical coefficient except x^p and y^p contains a factor of p. But p = 0 in a field of characteristic p and the result is verified.

For further study, an examination of more matrix examples could be carried out to determine the cardinality of the set of elements in an n x n matrix representation of a field with entries in $^I/_{(p)}$. That is, the 2 x 2 matrices of example 2.4 with entries in $^I/_{(3)}$ form a field of nine elements. Does the dimension of the matrix determine the number of elements in the field if the entries a_i, b_j are taken from $^I/_{(p)}$?

Another suggestion for additional study in the area of extensions is to be found in an article in the "Proceedings of the American Mathematical Society", volume 19, number 3, June, 1968, pages 701-706. This article by Edgar Enochs entitled "Totally Integrally Closed Rings", examines the concept of ring extensions which parallels the algebraic extension of a field. In fact, integral extensions in fields are the algebraic extensions. Using the definition that the characteristic of a ring is the smallest element "a" having the property that ax = 0 for all x in the ring and if ax = 0 implies a = 0 then the ring is of zero characteristic, integral extensions of rings of non-zero characteristic could provide an interesting study of extensions of finite rings.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Crawford, Albert L., "Lie Rings." Unpublished Master's thesis, Kansas State Teachers College, Emporia, 1966.

2. Enochs, Edgar, Totally Integrally Closed Rings, Providence, Rhode Island, American Mathematical Society, vol. 19, no. 3, June, 1968.

3. Herstein, I. N., Topics in Algebra, New York, Blaisdell Publishing Company, 1964.

4. Jacobson, Nathan, Lectures in Abstract Algebra, vol. III, Princeton, New Jersey, D. Van Nostrand, Inc., 1964.

5. Jacobson, Nathan, Structure of Rings, Providence, Rhode Island, American Mathematical Society, 1964.

6. MacDuffee, Cyrus Colton, An Introduction to Abstract Algebra, New York, Dover Publications, Inc. 1940.

7. Miller, Kenneth S., Elements of Modern Abstract Algebra, New York, Harper and Row, Publishers, 1958.