FIELD EXTENSIONS

by

BERNARD ROBERT MCDONALD

B. A., Park College, 1962

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF ARTS

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1964

Approved by:

Leonard D. Fuller

Major Professor

TABLE OF CONTENTS

INTRODUCTION 1

EXTENSION 5

CHARACTERISTIC 7

POLYNOMIAL DOMAIN 9

TRANSCENDENTAL FIELD EXTENSIONS 13

ALGEBRAIC FIELD EXTENSIONS 17

EXTENSION BY VALUATION 26

CONCLUSION 37

ACKNOWLEDGEMENT 39

REFERENCES 40

INTRODUCTION

A discussion of certain algebraic mathematical systems is presented in this report. A mathematical system may be viewed as a logical construct, a model fashioned from certain undefined concepts and certain specified properties.

Those systems under consideration in this report are characterized with respect to their elements, methods of combination of elements (operations), and element relationships. Symbolically these systems are designated as

$$(S;\ \theta_1,\ \theta_2,\ \theta_3,\ \ldots,\ \theta_n;\ R_1,\ R_2,\ R_3,\ \ldots,\ R_m)$$

where S denotes the set of elements

θ_i denotes an operation

R_j denotes a relationship between elements.

Specifically the discussion concerns the concept of 'field'; however, prior to the definition of a field several other systems are considered.

A group, denoted by $(G;\ 0;\ R)$, is defined as a set of elements G with a well-defined operation 0 and a relation R.

Under the relation R for all a and b contained in G:

(i.) Either aRb or $a \not R b$

(ii.) aRa always holds

(iii.) If aRb, then bRa

(iv.) If aRb and bRc, then aRc.

Under the operation @, a group satisfies the following postulates.

(i.) The system is closed under the operation.

(ii.) The operation is associative.

(iii.) There exists an element e such that for all a contained in G

a@e R e@a R a.

(iv.) For every element a contained in G there exists an a' contained in G such that

a@a' R a'@a R e.

If (G; @; R) also satifies

(v.) a@b R b@a

then (G; @; R) is called a commutative group.

Since the postive integers modulo a prime constitute a group under the operation of addition and the relation of equality, for simplicity, hereafter the relation R is to be referred to as =, the operation @ as +, and a' as -a. It should be remembered that these are merely symbolic representations of the concepts R, @, and a'.

A ring, denoted by (R; +, *; =), is a mathematical system composed of a set of elements R, two well-defined operations + and *, and a relation =.

A ring satisfies the following postulates.

(i.) The elements of R constitute a commutative group relative to the operation +.

(ii.) $a*(b*c) = (a*b)*c$.

(iii.) $a*(b + c) = a*b + a*c$ and

$(b + c)*a = b*a + c*a$.

If

(iv.) $a*b = b*a$

then the ring is called a commutative ring.

If there exists an element i such that

(v.) $a*i = i*a = a$

for all a, then the ring is called a ring with unity, denoted by (Ri; +, *; =).

A proper divisor of zero is now defined. If $a*b = e$ an $b \neq e$, then a is called a divisor of zero. If also $a \neq e$, then a and b are called proper divisors of zero.

An integral domain, denoted by (I; +, *; =), is defined as a commutative ring with unity which satisfies the postulate:

(i.) There are no proper divisors of zero.

Finally define a field, denoted by (F; +, *; =), as a commutative ring with unity which satisfies the postulate:

(i.) For every a contained in F, $a \neq e$, there exists an a^{-1} such that

$$a*a^{-1} = a^{-1}*a = i.$$

The element -a is called the additive inverse of the element a and the element a^{-1} is called the multiplicative inverse of the element a.

A field is also defined as a commutative ring with unity which satisfies the postulate:

(i.) The equation $ax = b$ $(a \neq e)$ has a solution for all a and b contained in $(F; +, *; =)$.

To illustrate the equivalence of these definitions it is sufficient to show that the postulate of the second definition implies the existence of a multiplicative inverse for every element a, $a \neq e$, contained in $(F; +, *; =)$. Since this is a commutative ring with unity there exists an x such that for $a \neq e$,

$$ax = i$$

where i is the unity element of the ring. Since this is a commutative ring, the a and x commute. Hence the x is the multiplicative inverse of a.

Examples of sets which under the operations of addition and multiplication and the relation equality satisfy the requirements for a field are:

(i.) All rational numbers

(ii.) All complex numbers

(iii.) All real numbers

(iv.) Sets of integers congruent modulo a prime integer

(v.) The set of numbers $a + b\sqrt{3}$ where a and b are rational numbers.

To conclude this section, define for a positive integer n:

$$na = a + a + \ldots + a \qquad \text{(n terms)}$$

$$-na = (-a) + (-a) + \ldots + (-a) \qquad \text{(n terms)}$$

$$a^n = a*a* \ldots *a \qquad \text{(n factors)}$$

$$a^{-n} = a^{-1}*a^{-1}* \ldots *a^{-1} \qquad \text{(n factors).}$$

EXTENSION

The concept 'set' is undefined when a mathematical system is constructed with operations and relations. Consequently many collections of elements, i.e. positive integers, rational numbers, 2x2 matrices, may form the 'set' satisfying the postulates of a system.

One selects a specific collection of elements to compose the 'set' of an algebraic system. One usually chooses a collection of elements because the collection has certain advantageous properties. However, through one's choice of a particular collection of elements, the system may lack other needed properties. Thus it often proves profitable, because of this absence of desired properties, to cause a mathematical system to 'grow'. Yet, it is essential to cause this growth in such a manner as not to lose any of the properties of the original system. A system is needed for which the properties of the antecedent system are maintained and certain desired properties have been added, i.e. an 'extension' is sought from the original system.

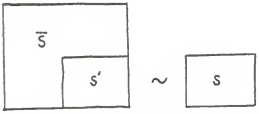
One says that $(\overline{S};\ \overline{\theta}_1,\ \overline{\theta}_2,\ldots,\overline{\theta}_n;\ \overline{R}_1,\ \overline{R}_2,\ldots,\ \overline{R}_m)$ constitutes an <u>extension</u> of $(S;\ \theta_1,\ \theta_2,\ldots,\ \theta_n;\ R_1,\ R_2,\ldots,\ R_m)$ if there exists a subset S' of $\overline{S}$ such that

$$(S';\ \overline{\theta}_1,\ \overline{\theta}_2,\ldots,\ \overline{\theta}_n;\ \overline{R}_1,\ \overline{R}_2,\ldots,\ \overline{R}_m)$$

is isomorphic to

$$(S;\ \theta_1,\ \theta_2,\ldots,\ \theta_n;\ R_1,\ R_2,\ldots,\ R_m).$$

Pictorially:



Since S' behaves in all instances identically as the original system S, for simplicity it is said that S is equal to S' and S is a subset of $\overline{S}$.

One might inquire as to the necessity of an extension of a system. Since this report is concerned with extensions of only a particular system, a field, let us consider an example in the rational field. Equations over the rational field such as

$$2x^2 - 4 = 0$$

and

$$x^2 + 1 = 0$$

possess no solutions in the rationals. Thus the polynomials cannot be reduced to linear factors over the rational field. The problem then is to extend the field under consideration to a 'larger' field from which solutions for the equations may be obtained.

CHARACTERISTIC[1]

With regard to the number of their elements, fields fall into two classifications. The given set of elements comprising the field may be either finite or infinite.

As an illustration of this difference, consider a field, $(F; +, *; =)$, and the subset of elements of $(F; +, *; =)$:

$$\ldots, -2(i), -1(i), 0(i) = e, 1(i), 2(i), \ldots$$

where for each $n(i)$, n is an integer multiple of the element i of $(F; +, *; =)$.[2] In general, for two positive integers, two relations may hold, either $j(i) = k(i)$ where $j > k$, or $j(i) = k(i)$ only if $j = k$.

If one considers the first case where

$$j(i) = k(i) \qquad j > k$$

then $j(i) - k(i) = e$

and $(j - k)(i) = e$.

This would imply that there exists some integer n such that $n(i) = e$. Simply select the smallest positive integer p for which $p(i) = e$ and call p the characteristic of $(F; +, *; =)$.

If a field has characteristic p, the field is finite.

---

[1]Cyrus Colton MacDuffee, An Introduction to Abstract Algebra, p. 156.

[2]Refer to page 3.

If, however,

$$j(i) = k(i) \qquad \text{only if} \quad j = k$$

then it is possible to write

$$j = k + m \cdot 0$$

and $$j - k = m \cdot 0.$$

Thus, j - k is a multiple of the non-negative integer 0, i.e. j is congruent to k modulo 0. If (F; +, *; =) satisfies this second condition, then (F; +, *; =) is said to have characteristic 0. In this second case some authors may refer to this characteristic as 'infinity'.[3] If a field has characteristic 0, the field has an infinite number of elements.

Theorem 1.1 If the characteristic of a field is p, then p is a prime.

Clearly the characteristic cannot be 1 for $1(i) = i \neq e$.

Assume p is composite. Then p may be written

$$p = p_1 p_2 \qquad \text{where} \quad p_1 > 1,\ p_2 > 1$$

$$p(i) = p_1(i)p_2(i) = e.$$

Now assume $p_1(i) \neq e$ and $p_2(i) \neq e$. If this is true, then $p_1(i)$ and $p_2(i)$ are in the multiplicative group, with e omitted, of (F; +, *; =). This group is closed, hence the product $p_1(i)p_2(i)$ is in the group. Therefore $p_1(i)p_2(i) \neq e$.

This is a contradiction, thus either

---

[3] Garrett Birkhoff and Saunders MacLane, A Survey of Modern Algebra, pp. 391-92.

$$p_1(i) = e$$

or $$p_2(i) = e.$$

This contradicts the definition of p. Hence p is neither composite nor one. Thus p is a prime.

POLYNOMIAL DOMAIN

Prior to the discussion of field extensions, it is necessary to consider the mathematical system formed from the polynomials

$$(1) \qquad a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n \qquad n = 0, 1, 2, \ldots$$

where a_i is an element of $(F; +, *; =)$

x is an indeterminant that commutes with the elements of the field.

It is also assumed that the 'powers' of x obey the ordinary laws of exponents.

If j is the highest power of x in the polynomial such that $a_j \neq e$ and for all k, where $k > j$, $a_k = e$, then j is called the degree of the polynomial.

If one considers the mathematical system constructed from rational operations with polynomials of the form (1), one notes that in addition and multiplication of polynomials only the coefficients of the indeterminants are affected. Thus, if multiplication and addition are properly defined, it is

sufficient to concern oneself with operations involving the ordered sets[4]

(2) $A = (a_0, a_1, a_2, \ldots, a_n) \quad n = 0, 1, 2, \ldots$

where each a_i of the ordered set (2) is the a_i of the polynomial (1).

If A and B are ordered sets of the form (2), then A is said to equal B,

$$(a_0, a_1, a_2, \ldots, a_n) = (b_0, b_1, b_2, \ldots, b_m)$$

where $m > n$, if $a_i = b_i$ for $i = 0, 1, 2, \ldots, n$ and $b_i = e$ for $i > n$.

If one considers any collection of ordered sets of the form (2), one may consider them to have the same number of elements since e's may be placed at the right as desired.

Define addition of A + B as

$$(a_0, a_1, a_2, \ldots, a_n) + (b_0, b_1, b_2, \ldots, b_n) =$$

$$(a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Define multiplication, AB, as

$$(a_0, a_1, a_2, \ldots, a_n)(b_0, b_1, b_2, \ldots, b_n) =$$

$$(c_0, c_1, c_2, \ldots, c_k) \qquad k = m + n$$

where $$c_i = \sum_{r+s=i} a_r b_s.$$

---

[4]MacDuffee, op. cit., pp. 158-161.

This system of ordered sets is denoted $(F[x]; +, *; =)$.

Theorem 1.2 The system $(F[x]; +, *; =)$ is an integral domain.

Consider first the operation of addition.

(i.) By definition the system is closed.

(ii.) The system is associative since the elements of $(F; +, *; =)$ are associative under $+$.

(iii.) The system is commutative since the elements of $(F;+, *; =)$ are commutative.

(iv.) The inverse $-A$ of $A = (a_0, a_1, \ldots, a_n)$ is $(-a_0, -a_1, \ldots, -a_n)$.

(v.) The unit element of $+$ is $(e, e, e, \ldots, e)$.

Under the operation of multiplication:

(i.) Multiplication is associative $(AB)C = A(BC)$:

$$(a_0, a_1, a_2, \ldots, a_n)(b_0, b_1, b_2, \ldots, b_m) =$$

$$(d_0, d_1, d_2, \ldots, d_{m+n})$$

where $$d_i = \sum_{r+s=i} a_r b_s.$$

Let

$$(d_0, d_1, d_2, \ldots, d_{m+n})(c_0, c_1, c_2, \ldots, c_h) =$$

$$(e_0, e_1, e_2, \ldots, e_{h+m+n})$$

$$e_j = \sum_{p+q=j} d_p c_q = \sum_{p+q=j} \left(\sum_{r+s=p} a_r b_s \right) c_q.$$

Since one is summing over a finite collection of elements and the associative and generalized distributive laws hold for (F; +, *; =), then

$$e_j = \sum_{r+s+p=j} a_r b_s c_q .$$

If one now reassociates and separates the products of summations, one has A(BC). Thus multiplication is associative.

(ii.) The identity for multiplication is

$$(i, e, e, \ldots, e).$$

$$(a_0, a_1, a_2, \ldots, a_n)(i, e, e, e, \ldots, e) =$$

$$(c_0, c_1, c_2, \ldots, c_m)$$

where

$$c_i = \sum_{r+s=i} a_r K_s$$

with

$$K_0 = i$$

$$K_s = e \qquad \text{for } s \neq 0.$$

Hence $c_i = a_i$.

(iii.) The distributive law is valid.

Let A(B + C) = D. Then

$$d_i = \sum_{r+s=i} a_r (b_s + c_s) = \sum_{r+s=i} a_r b_s + \sum_{r+s=i} a_r c_s .$$

Now let AB + AC = E. Then

$$e_i = \sum_{r+s=i} a_r b_s + \sum_{r+s=i} a_r c_s .$$

Hence $e_i = d_i$.

(iv.) Multiplication is commutative by definition.

(v.) The system (F[x]; +, *; =) has no proper divisors of zero.

To demonstrate this final property consider the ordered set denoted by a of the form (2). If A is not equal to the identity of addition, then the ordered set must contain at least one element a_i such that $a_i \neq e$. Likewise is B is not equal to the identity for addition, then the ordered set denoted by B must contain some $b_j \neq e$. Then the product AB must contain at least the element $a_i b_j$. But a_i b_j are taken from (F; +, *; =), therefore $a_i b_j \neq e$. Hence there are no proper divisors of zero.

Therefore (F[x]; +, *; =) is an integral domain. The system (F[x]; +, *; =) is defined as the polynomial domain of (F; +, *; =).

TRANSCENDENTAL FIELD EXTENSIONS[5]

Consider the field (F; +, *; =) and the elements A, B, C, . . . of its polynomial domain (F[x]; +, *; =). Form the ordered pairs (A,B) of the elements of the polynomial domain subject to the condition that $B \neq e'$, where

---

[5] J. B. Roberts, The Real Number in an Algebraic Setting, pp. 41-42.
MacDuffee, op. cit., pp. 153-155, 180-181.
Birhoff, op. cit., pp. 39-43.

e' is the additive identity of the polynomial domain.

Equality for these ordered pairs is defined as

$$(A,B) = (C,D) \text{ if and only if } AD = BC.$$

Theorem 2.1 Equality of ordered pairs of a polynomial domain satisfies the requirement of the relation R of a group.

It is obvious from the definition of equality that $(A,B) = (A,B)$ and that if $(A,B) = (C,D)$ then $(C,D) = (A,B)$. To demonstrate the validity of the transitivity property assume that $(A,B) = (C,D)$ and that $(C,D) = (E,F)$, i.e. that $AD = BC$ and $CF = DE$. After multiplication by F and B, respectively, these equations become $ADF = BCF$ and $BCF = BDE$. Consequently, $ADF = BDE$, and since these are elements of an integral domain which has no proper divisors of zero

$$ADF - BDE = D(AF - BE) = e'$$

$$AF - BE = e'$$

$$AF = BE.$$

Therefore $(A,B) = (E,F)$.

Addition of these ordered couples is defined as

$$(A,B) + (C,D) = (AD + BC, BD) \qquad BD \neq e'.$$

Multiplication is defined as

$$(A,B)(C,D) = (AC,BD) \qquad BD \neq e'.$$

The system formed from the set of ordered pairs under the above definitions for equality, addition, and multiplication is characterized as $(QF; +, *; =)$.

Theorem 2.3 The mathematical system (QF; +, *; =) is a field.[6]

Consider the postulates for a field under addition:

(i.) In (A,B) and (C,D) one has $B \neq e'$ and $D \neq e'$, so that $BD \neq e'$. Hence the element (AD + BC, BD) exists. The system is closed. If (A,B) = (A',B') and (C,D) = (C',D'), then AB' = BA' and CD' = DC'. One has

$$\begin{aligned}(AD + BC)B'D' &= (AB')DD' + BB'(CD') \\ &= (BA')DD' + BB'(DC') \\ &= BD(A'D' + B'C')\end{aligned}$$

which implies

$$(AD + BC, DB) = (A'D' + B'C', B'D')$$

and the operation is well defined.

(ii.) The commutative property:

$$\begin{aligned}(A,B) + (C,D) &= (AD + BC, BD) \\ &= (CB + DA, BD) \\ &= (C,D) + (A,B)\end{aligned}$$

(iii.) The associative property:

$$\begin{aligned}[(A,B) + (C,D)] + (E,F) &= \\ &= (AD + BC, BD) + (E,F) \\ &= [(AD + BC)F + BDE, B(DF)] \\ &= [A(DE) + B(CF + DE), BDF] \\ &= (A,B) + [(CF + DE), DF] \\ &= (A,B) + [(C,D) + (E,F)].\end{aligned}$$

---

[6] B. M. Stewart, Theory of Numbers, pp. 216-217.

(iv.) The inverse of addition for (A,B) is (-A,B).

(v.) The additive identity is (e',A).

Consider the postulates for a field under multiplication:

(i.) The operation is closed. If (A,B) = (A',B') and (C,D) = (C',D'), so that AB' = BA' and CD' = DC', then ACB'D' = BDA'C'. This implies that (AC,BD) = (A'C',B'D'). Hence (A,B)(C,D) = (A',B')(C',D'). Thus the operation is well defined.

(ii.) The commutative property:

ACDB = BDCA implies that (AC, BD) = (CA, DB).

Hence

$$(A,B)(C,D) = (C,D)(A,B).$$

(iii.) The associative property:

Consider the quantity ABCDEF. Under multiplication in (F[x]; +, *; =) this quantity is expressed as

$$[(AC)E][B(DF)] = [(BD)F][A(CE)].$$

Which in (QF; +, *; =) becomes

$$(AC,BD)(E,F) = (A,B)(CE,DF)$$

$$[(A,B)(C,D)](E,F) = (A,B)[(C,D)(E,F)].$$

(iv.) The identity for multiplication is (A,A) where $A \neq e'$.

(v.) The multiplicative inverse of (A,B) is (B,A) where $A \neq e'$.

Finally if one considers the operations together, one notes that within the system (QF; +, *; =) the distributive law holds.

Consider in (F[x]; +, *; =) the quantity (AD + BC)EBFDF which is expressed as

$$(AD + BC)E(BF)(DF) = (BD)F[AE(DF) + BF(CE)]$$

which is written in terms of ordered pairs in (QF; +, *; =) as

$$[(AD + BC, BD)](E,F) = (AE,BF) + (CE,DF)$$

$$[(A,B) + (C,D)](E,F) = (A,B)(E,F) + (C,D)(E,F).$$

Therefore (QF; +, *; =) is a field. The system (QF; +, *; =) is called the quotient field of (F; +, *; =). The method of passing from (F; +, *; =) to (F[x]; +, *; =) and then to (QF; +, *; =) is characterized as a transcendental extension of (F; +, *; =).

The elements a, b, c, . . . of (F; +, *; =) under a transcendental extension correspond to the subset (A', I), (B',I), (C',I), . . . of (QF; +, *; =) for which

$$I = (i, e, e, e, \ldots)$$

$$A' = (a, e, e, e, \ldots)$$

$$B' = (b, e, e, e, \ldots)$$

$$C' = (c, e, e, e, \ldots).$$

ALGEBRAIC FIELD EXTENSIONS

An ideal, denoted by Id-F[x], of (F[x]; +, *; =) is defined as the set of all numbers of (F[x]; +, *; =) such that:

(i.) If a and b are contained in Id-F[x], then
a - b is contained in Id-F[x].

(ii.) If r is contained in (F[x]; +, *; =) and
a is contained in Id-F[x], then ar is
contained in Id-F[x].

One also says that two numbers a and b of (F[x]; +, *; =) are congruent modulo Id-F[x] if their difference a - b is in Id-F[x], symbolically:

$$a \stackrel{\circ}{=} b \mod \text{Id-F[x]} \quad \text{iff} \quad a - b = m$$

where m is contained in Id-F[x].

It is noted that Id-F[x] forms a commutative group under the operation of addition.

Theorem 3.1 The relation congruence modulo Id-F[x] satisfies the relation R.[7]

(i.) a - b is either in Id-F[x] or it is not.

(ii.) If a is contained in Id-F[x], then a - a = e.
Hence e is contained in Id-F[x]. Therefore

$$a \stackrel{\circ}{=} a \mod \text{Id-F[x]}$$

(iii.) If m is contained in Id-F[x], then e - m
is contained in Id-F[x] and -m is in Id-F[x].
Therefore, if

$$a \stackrel{\circ}{=} b \mod \text{Id-F[x]}$$

---

[7]Refer to definition of relation R, page 1.

then

$$a - b = m \qquad \text{where } m \text{ is in Id-F[x]}$$

$$a - m = b$$

$$-m = b - a.$$

Hence

$$b \triangleq a \mod \text{Id-F[x]}.$$

(iv.) If $a \triangleq b \mod \text{Id-F[x]}$ and $b \triangleq c \mod \text{Id-F[x]}$, then

$$a - b = m_1$$

$$b - c = m_2 \qquad \text{where } m_1 \text{ and } m_2 \text{ are in Id-F[x].}$$

The system Id-F[x] is closed under addition since Id-F[x] is a group; hence $m_1 + m_2$ is contained in Id-F[x].

$$a - c = m_1 + m_2$$

$$a \triangleq c \mod \text{Id-F[x]}.$$

Consider the set of all $f_i(x)$ of $(F[x]; +, *; =)$. Select from among the set of elements $f_i(x)$ a set of elements $f_i'(x)$ such that:

(i.) The set of elements $f_i'(x)$ are incongruent modulo Id-F[x].

(ii.) Every $f_i(x)$ is congruent to one $f_i'(x)$.

The set of $f_i'(x)$ is called a <u>complete set of residues</u> modulo Id-F[x] and is denoted by $(F[x]; +, *; =)/\text{Id-F[x]}$.

Prior to the actual extension of a field using algebraic techniques, consider more fully Id-F[x].

An ideal Id-F[x] is called principal if the ideal is generated by a single element, i.e. if Id-F[x] is equal to the set of all ra where:

(i.) The element a is a fixed element of Id-F[x].

(ii.) The element r is contained in (F[x]; +, *; =).

The principal ideal Id-F[x] is said to be generated by the fixed element a, characterized as (a).

Theorem 3.2 Every ideal in (F[x]; +, *; =) is principal.[8]

Let A be an ideal in (F[x]; +, *; =). If A is equal to the zero ideal, then A = (e). If A is not equal to the zero ideal, then A contains polynomials not identically zero.

Let f(x) be such a polynomial and of minimum degree in A . Let g(x) be any polynomial of A. One can write

$$g(x) = q(x)f(x) + r(x)$$

where the degree of r(x) is less than the degree of f(x) or r(x) = e.

Since f(x) is contained in A, q(x)f(x) is contained in A. Also g(x) is in A. Therefore g(x) - q(x)f(x) is contained in A. This implies that r(x) is contained in A.

---

[8]The proof of this theorem is taken from the lectures of Assistant Professor Richard L. Yates, Theory of Rings and Ideals, Kansas State University, Fall Semester, 1963.

However, if $r(x) \neq e$, then this contradicts the definition of $f(x)$ since $f(x)$ is of minimum degree. Hence $r(x) = e$ and $g(x) = q(x)f(x)$. Therefore A is generated by $f(x)$ and A is principal.

A polynomial $p(x)$ in $(F[x]; +, *; =)$ is called irreducible or prime if $p(x)$ cannot be expressed as a product of two or more factors of degree greater than zero and less than $p(x)$ in $(F[x]; +, *; =)$.

An ideal M of $(F[x]; +, *; =)$ is said to be maximal if when M is contained in N and N is an ideal in $(F[x]; +, *; =)$, then $N = (F[x]; +, *; =)$.

Theorem 3.3 Ideals generated by prime polynomials in $(F[x]; +, *; =)$ are maximal.

Consider $f(x)$ where $f(x)$ is not contained in the ideal generated by the prime polynomial $p(x)$, denoted by $(p(x))$. Then there exist polynomials $t(x)$ and $s(x)$ in $(F[x]; +, *; =)$ such that

$$f(x)t(x) + s(x)p(x) = i.$$

Hence i is in the ideal generated by both $p(x)$ and $f(x)$. Since the ideal is closed under multiplication by all of the elements of $(F[x]; +, *; =)$, and $g(x)i = g(x)$, for all $g(x)$ in $(F[x]; +, *; =)$, the ideal generated by both $p(x)$ and $f(x)$ is equal to $(F[x]; +, *; =)$. Therefore $(p(x))$ is maximal.

Theorem 3.4 If M is a maximal ideal generated by a prime polynomial in $(F[x]; +, *; =)$, then $(F[x]; +, *; =)/M$ is a field.[9]

The first part of this proof consists of a demonstration that $(F[x]; +, *; =)/M$ is a commutative ring with unity.

(i.) Since the associative, commutative, and distributive properties are valid in $(F[x]; +, *; =)$, the properties are valid in $(F[x]; +, *; =)/M$.

(ii.) Since $(F[x]; +, *; =)$ has identities for addition and multiplication so also will $(F[x]; +, *; =)/M$. These are the residue classes of which i and e are members. As an example of this last statement, consider the case involving the identity for multiplication. Suppose for a and k contained in $(F[x]; +, *; =)$

$$ak \triangleq a \mod M$$

where $k \neq i$. Then

$$ak \triangleq ai \mod M.$$

Since M is an ideal generated by a prime polynomial, from the properties of congruences,

---

[9]The first section of this proof is taken from MacDuffee, op. cit., pp. 165-166. The second section is discussed in Neal H. McCoy, Rings and Ideals, pp. 81-82.

the a's may be cancelled and

$$k \triangleq i \mod M.$$

Hence k and i are contained in the same residue class.

(iii.) Since $(F[x]; +, *; =)$ possesses an additive inverse for each element a, so also does $(F[x]; +, *; =)/M$. The additive inverse for the residue class containing a is the residue class containing -a.

Secondly, it remains to be shown that the equation

$$ax = b \qquad (a \neq e)$$

where a and b are contained in $(F[x]; +, *; =)/M$ has a unique solution x contained in $(F[x]; +, *; =)/M$.

Let

$$a \not\triangleq e \mod M.$$

Therefore $a \neq e$ in $(F[x]; +, *; =)$.

Then the ideal generated by a and the ideal M must equal $(F[x]; +, *; =)$, since M is maximal. Each element of the ideal generated by M and a may be expressed as

$$m + ra$$

where m is contained in M and r is contained in $(F[x]; +, *; =)$.

Hence

$$i = m_1 + r_1 a$$

$$a = m_1 a + r_1 a^2.$$

Therefore

$$a \triangleq r_1 a^2 \mod M.$$

If $a^2 = e$, then $a = e$, and hence one has a contradiction. Hence $a^2 \neq e$.

Now let N equal the set of all ax such that x is contained in (F[x]; +, *; =). Then N is an ideal in (F[x]; +, *; =) and N is not contained in M since a is not contained in M.

Therefore the set generated by the ideals M and N, i.e. the set of all linear combinations of elements of M and N with coefficients in (F[x]; +, *; =), is an ideal and must equal (F[x]; +, *; =). Then any element of (F[x]; +, *; =) may be written in the form

$$m + ax$$

with m contained in M and x contained in (F[x]; +, *; =). This implies

$$b = m_2 + ax_1$$

$$b - ax_1 = m_2.$$

Hence

$$b \triangleq ax_1 \mod M$$

and thus $b = ax_1$ in $(F[x]; +, *; =)/M$. Therefore $(F[x]; +, *; =)/M$ is a field.

As an example of this method of field extension, consider

the field of integers modulo 2, its polynomial domain, and the irreducible polynomial $x^2 + x + 1$. The system $(F[x]; +, *; =)/(x^2 + x + 1)$, where $(F[x]; +, *; =)$ is the set of all polynomials in an indeterminant x with coefficients in I_2, would consist of the following polynomials:

$$1$$

$$0$$

$$x + 1$$

$$x.$$

By constructing addition and multiplication tables one observes that these four elements form a field which contains I_2 as a proper subfield, and hence one has an algebraic extension of I_2.

(addition)

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

(multiplication)

*	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	x + 1	1
x + 1	0	x + 1	1	x

As a second example of this method, consider the field of real numbers, its polynomial domain, and the irreducible equation $x^2 + 1 = 0$. The system

$(F[x]; +, *; =)/(x^2 + 1)$, where $(F[x]; +, *; =)$ represents the polynomial domain of the real number system, consists of all polynomials of the form

$$ax + b$$

where a and b are real numbers. This system forms a field in which the real numbers are a proper subset. One has an extension of the real field; in fact, one has actually constructed the complex field.

The elements elements a, b, c, . . . of $(F; +, *; =)$ under an algebraic extension correspond to the residue classes which contain a, b, c, . . . as polynomials of zero degree from $(F[x]; +, *; =)$.

An algebraic extension of a field modulo and irreducible polynomial p(x) is isomorphic to the set of all rational functions of r where r is a root of p(x). For a discussion of this method of approach consult An Introduction to Abstract Algebra by MacDuffee.

EXTENSION BY VALUATION

A field $(F; +, *; =)$ is called ordered if the property of positiveness ($> e$) is defined for its elements and if the field satisfies the following properties:[10]

---

[10] B. L. Van Der Waerden, Modern Algebra, Vol. 1, p. 209.

(i.) For every element a contained in
(F; +, *; =) just one of the relations
$a = e$, $a > e$, $-a > e$ is valid.

(ii.) If $a > e$ and $b > e$, then $a + b > e$
and $ab > e$.

If $-a > e$, a is said to be negative; otherwise, for $a \neq e$, a is called positive.

The ordered field is characterized by $(F; +, *; =, >)$.

If $a + (-b) = a - b > e$, then one says that $a > b$ which is read "a is greater than b". This relation between a and b is also written $b < a$ and is read "b is less than a". The sysbol $a \geq b$ is to be read "a is greater than or equal to b" and is interpeted as either $a > b$ or $a = b$ and never both. The analagous situation is true for $b \leq a$.

One can see that the rationals satisfy the postulates of an ordered field. However, if one considers the field I_5 (integers modulo 5) and the element 3, then from above if I_5 is to be an ordered field either $-3 > 0$ or $3 > 0$.

If $3 > 0$, then

$$3 + 3 = 1 > 0$$

and

$$3 + 1 = 4 > 0.$$

However, $4 + 1 = 0$. Thus $3 \not> 0$.

If $-3 > 0$, then

$$(-3)(-3) = 4 > 0$$

and $$(4)(4) = 1 > 0.$$

However, again $4 + 1 = 0$. Thus $-3 \not> 0$. Clearly $3 \neq 0$, therefore I_5 is not an ordered field.

Further one may note that the identity for multiplication $i > e$, so that every sum $ni = i + i + \ldots + i > e$ for an order field. One concludes therefore that there does not exist a p such that $pi = e$, i.e. the characteristic of an ordered field cannot be prime. Hence the ordered fields are of characteristic 0.

Consider an ordered field $(F; +, *; =, >)$ and a non-empty set of elements M contained in $(F; +, *; =, >)$. If there exists an element a contained in $(F; +, *; =, >)$ such that for all m contained in M, $m < a$, then a is called an upper bound of M. If a is less than all other upper bounds of M, then a is called the least upper bound of M. Likewise, if there exists an element b contained in $(F; +, *; =, >)$ such that for all m contained in M, $b < m$, then b is called a lower bound of M. If b is greater than all other lower bounds of M, then b is called the greatest lower bound of M. If M has an upper bound, M is said to be bounded above, and if M has a lower bound, M is said to be bounded below.[11]

---

[11] Van Der Waerden, op. cit., pp. 212-215.

Finally, a field is said to have a valuation if a function $\emptyset(a)$ is defined for the elements a and b of the field such that:

(i.) $\emptyset(a)$ is an element of an ordered field $(F; +, *; =, >)$.

(ii.) $\emptyset(a) > e'$ for $a \neq e$, $\emptyset(e) = e'$ where e' is the additive identity of $(F; +, *; =, >)$.

(iii.) $\emptyset(ab) = \emptyset(a)\emptyset(b)$.

(iv.) $\emptyset(a + b) \leq \emptyset(a) + \emptyset(b)$.

One can see from (ii.) and (iii.) that if i' is the multiplicative identity of $(F; +, *; =, >)$, then

$$\emptyset(i) = i' \quad \emptyset(-i) = i' \quad \emptyset(a) = \emptyset(-a),$$

and from (iv.)

$$\emptyset(a + b) \leq \emptyset(a) + \emptyset(b)$$

$$\emptyset(a + b) - \emptyset(a) \leq \emptyset(b).$$

Replacing b by c - a, this becomes

$$\emptyset(c) - \emptyset(a) \leq \emptyset(c - a).$$

Consider an ordered field $(F; +, *; =, >)$ and a sequence of its elements. Define an infinite sequence of elements $a_1, a_2, a_3, \ldots$ in the ordered field as a regular (Cauchy or fundamental) sequence, denoted by $\{a_I\}$, if, for every positive element g of $(F; +, *; =, >)$ there exists an integer n, such that

$$\emptyset(a_p - a_q) < g \qquad \text{for} \qquad p > n,\ q > n.$$

Two regular sequences $\{a_p\}$ and $\{b_p\}$ are said to be equal if, for every positive g, there exists a positive integer n, such that

$$\emptyset(a_p - b_p) < g \qquad \text{for } p > n.$$

Theorem 4.1 Every regular sequence is bounded above.

Consider

$$\emptyset(a_p - a_q) < g \qquad \text{for } p > n,\ q > n.$$

Adding $\emptyset(a_q)$, one has

$$\emptyset(a_q) + \emptyset(a_p - a_q) < \emptyset(a_q) + g$$

$$\emptyset(a_p) = \emptyset(a_q + a_p - a_q) \leq \emptyset(a_q) + \emptyset(a_p - a_q) < \emptyset(a_q) + g.$$

Let $q = n + 1$. One has

$$\emptyset(a_p) \leq \emptyset(a_q) + \emptyset(a_p - a_q) < \emptyset(a_{n+1}) + g = N \qquad \text{for } p > n.$$

Thus for every g there exists a bound $N = \emptyset(a_{n+1}) + g$ such that for $p > n$

$$\emptyset(a_p) < N.$$

The sums and products of regular sequences are defined as

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} = \{c_n\}$$

and

$$\{a_n\}\{b_n\} = \{a_n b_n\} = \{d_n\}.$$

Theorem 4.2 The sums and products of regular sequences are themselves regular sequences.

For every g there exists an n_1 such that

$$\emptyset(a_p - a_q) < 1/2\ g \qquad \text{for } p > n_1,\ q > n_1$$

and an n_2 such that

$$\emptyset(b_p - b_q) < 1/2\ g \qquad \text{for } p > n_2,\ q > n_2.$$

Let n be the larger of the numbers n_1 and n_2. Then

$$\emptyset[(a_p + b_p) - (a_q + b_q)] = \emptyset[(a_p - a_q) + (b_p - b_q)]$$

$$\leq \emptyset(a_p - a_q) + \emptyset(b_p - b_q) < g$$

for $p > n$ and $q > n$.

That is

$$\emptyset(c_p - c_q) < g \qquad \text{for } p > n,\ q > n.$$

Likewise, there exist N_1 and N_2 such that

$$\emptyset(a_p) < N_1 \qquad \text{for } p > n_1$$

$$\emptyset(b_p) < N_2 \qquad \text{for } p > n_2.$$

Further for every g there exists $n' \geq n_2$ and $n'' \geq n_1$ such that

(1) $$\emptyset(a_p - a_q) < g/2N_2 \qquad \text{for } p > n',\ q > n'$$

(2) $$\emptyset(b_p - b_q) < g/2N_1 \qquad \text{for } p > n'',\ q > n''.$$

Multiplication of (1) and (2) by $\emptyset(b_p)$ and

$\emptyset(a_p)$ respectively yields

$$\emptyset(a_p b_p - a_q b_p) < g/2 \qquad \text{for } p > n',\ q > n'$$

$$\emptyset(a_q b_p - a_q b_q) < g/2 \qquad \text{for } p > n'',\ q > n''$$

which, upon addition, gives

$$\emptyset(a_p b_p - a_q b_q) < g \qquad \text{for } p > n,\ q > n$$

where n is the greater of n' and n".

Thus, the sums and products of regular sequences are closed.

Having defined addition and multiplication for the regular sequences and noting their construction from elements of an ordered field, consider the mathematical system generated by these sequences under addition and multiplication.[12]

The sequences form a commutative group under the operation of addition:

$$\begin{aligned}
\text{(i.)}\quad \{a_p\} + \left(\{b_p\} + \{c_p\}\right) &= \{a_p\} + \{b_p + c_p\} \\
&= \{a_p + (b_p + c_p)\} \\
&= \{(a_p + b_p) + c_p\} \\
&= \{a_p + b_p\} + \{c_p\} \\
&= \left(\{a_p\} + \{b_p\}\right) + \{c_p\} .
\end{aligned}$$

---

[12] The following section is discussed in MacDuffee, op. cit., pp. 185-186.

(ii.) The additive identity is $\{e\}$. From the definition of equality of sequences, as is noted below, the sequence representing the additive identity is not unique.

(iii.) The inverse of $\{a_p\}$ is $\{-a_p\}$.

(iv.) The sequences are commutative.

$$\{a_p\} + \{b_p\} = \{a_p + b_p\}$$
$$= \{b_p + a_p\}$$
$$= \{b_p\} + \{a_p\}$$

The sequence forming the additive identity is called the zero sequence. A sequence $\{a_p\}$ is said to be equal to zero if for every positive g there exists an integer n such that

$$\emptyset(a_p) < g \qquad \text{for } p > n.$$

Under multiplication the sequences which are not equal to zero form a commutative group.

(i.) If $\{a_p\}$ and $\{b_p\}$ are not equal to zero, then there exist $n_1 > e$, $n_2 > e$ such that

$$\emptyset(a_p) \geq n_1 \qquad \emptyset(b_p) \geq n_2 \qquad \text{for } p > n.$$

Then

$$\emptyset(a_p b_p) \geq n_1 n_2 > e$$

which implies

$$\{a_p b_p\} \neq \{e\}.$$

(ii.) Associativity and commutativity for sequences essentially involves noting whether the elements a_p and b_p obey these postulates. Since a_p and b_p are elements taken from a field, the associate and commutative properties follow.

(iii.) The multiplicative identity is $\{i\} = (i, i, i, \ldots)$. As was noted with with the additive identity, the multiplicative identity may have elements different from i.

(iv.) The inverse for multiplication is defined in the following manner: Let $\emptyset(a_p) \geq N_1 > e$, for $p > n$. Define $b_p = e$ for $p \leq n$, $b_p = i/a_p$ for $p > n$.

Then

$$\{a_p\}\{b_p\} = (e, e, e, \ldots, i, i, \ldots).$$

If $\{b_p\}$ is regular and not equal to zero, one is done. To demonstrate that $\{b_p\}$ is regular, consider:

$$\emptyset(a_q - a_p) = \emptyset(a_p a_q [i/a_p - i/a_q])$$

$$= \phi(a_p a_q)\phi(i/a_p - i/a_q) \leq gN_1^2$$

for p and $q > n_1 \geq n$.

Then divide by $\phi(a_p a_q) \geq N_1^2$. One has on the right hand side

$$\phi(i/a_p - i/a_q) \leq g \qquad \text{for } p, q > n_1.$$

Secondly, if $\{b_p\}$ were zero, then

$$\{a_p\}\{b_p\} = \{e\}.$$

However, this is not the case; hence

$$\{b_p\} \neq \text{zero}.$$

To complete the examination of this system, it remains only to note in what manner the operations may be combined, i.e. the validity of the distributive law.

$$\begin{aligned}\left(\{a_p\} + \{b_p\}\right)\{c_p\} &= \{(a_p + b_p)c_p\} \\ &= \{a_p c_p + b_p c_p\} \\ &= \{a_p c_p\} + \{b_p c_p\} \\ &= \{a_p\}\{c_p\} + \{b_p\}\{c_p\}.\end{aligned}$$

Since the elements commute, the right distributive law is valid.

Hence, from the above results, it follows that regular

sequences constructed from the elements of an ordered field under a valuation form a field. It should also be noted that the sequences of the form (a, a, a, . . .) are isomorphic with the original field (F; +, *; =, >) under the correspondence:

$$a \longleftrightarrow (a, a, a, \ldots)$$

$$b \longleftrightarrow (b, b, b, \ldots)$$

$$a + b \longleftrightarrow (a + b, a + b, a + b, \ldots)$$

$$ab \longleftrightarrow (ab, ab, ab, \ldots).$$

Hence, an extension of (F; +, *; =, >) has been constructed.

Examples of functions on an ordered field, fulfilling the properties of a valuation, are:

(i.) $\emptyset(a) = |a|$ where $|a|$ is the absolute value of a. If this valuation is applied to the rationals, the real field is constructed.

In this case, one defines a sequence of rational numbers such that for every positive rational number g, there is a positive integer n and

$$|a_p - a_q| < g \qquad \text{for } p > n,\ q > n.$$

(ii.) The trivial valuation $\emptyset(a) = i'$ for $a \neq e$, and $\emptyset(e) = e'$. In this example, the sequences after the first finite number of elements would 'settle down' to a single repeating element.

(iii.) If $(F; +, *; =, >)$ is the field of rationals and p is a fixed prime, one can write every rational in the form $a = (s/t)p^n$ where s and t are prime to p.

Define: $\emptyset_p(a) = p^{-n}$ for $a \neq e$, and $\emptyset_p(e) = e'$.

The use of this valuation will construct the system known as the p-adic field.

(iv.) If $(F; +, *; =, >)$ is the field of rationals, one can define:

$$\emptyset(a) = |a|^k \quad \text{where} \quad 0 < k \leq 1.$$

CONCLUSION

The purpose of this report is to outline briefly several methods of extending a field to a larger field. This larger field either contains the original field as a proper subset or contains a subfield which is isomorphic to the original field.

The transcendental extension involves initially the extension of a field to its polynomial domain. It is then noted that ordered pairs of elements of the polynomial domain, with appropriate definitions for equality and operations, formed a field containing the original

field as a proper subset.

In a second method of approach, the field is again extended to a polynomial domain. This domain is then reduced modulo any irreducible polynomial contained in the polynomial domain into a set of residue classes. These residue classes, with definitions for addition, multiplication, and equality, form a field.

Finally, the elements of an ordered field are arranged into regular sequences. Here it is again observed that, under appropriate definitions for operations and relations, the set of sequences behave as a field.

ACKNOWLEDGEMENT

The writer wishes to express his sincere appreciation to Professor L. E. Fuller for his guidance and to J. G. McDonald for her patience in the preparation of this report.

REFERENCES

Albert, Adrain. Modern Higher Algebra. Chicago, Illinois: University of Chicago Press, 1936.

Birkhoff, Garrett, and Saunders MacLane. A Survey of Modern Algebra. New York: MacMillan, 1960.

MacDuffee, Cyrus Colton. An Introduction to Abstract Algebra. New York: John Wiley and Sons, 1959.

McCoy, Neal H. Rings and Ideals. (The Mathematical Association of America). Menasha, Wisconsin: Beorge Banta Company, Inc., 1962.

Roberts, J. B. The Real Number System in an Algebraic Setting. San Francisco and London: W. H. Freeman and Co., 1962.

Sawyer, W. W. A Concrete Approach to Abstract Algebra . San Francisco and London: W. H. Freeman and Co., 1963.

Stewart, B. M. Theory of Numbers. New York: MacMillan, 1962.

Van Der Waerden, B. L. Modern Algebra, Volume 1. New York: Frederick Ugar Co., 1949.

FIELD EXTENSIONS

by

BERNARD ROBERT MCDONALD

B. A., Park College, 1962

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF ARTS

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1964

Though an algebraic system may possess desirable properties, in certain circumstances a given system may lack qualities necessary for special purposes. Such is the case when one is seeking a solution to the equation $x^2 + 1 = 0$ and one is working only with the rational field of numbers. It is often necessary to extend the system to a 'larger' system. This extension, however, must preserve the properties of the original system. Thus the second constructed-system either contains the initial system as a proper subset or contains a subset isomorphic to the initial system.

The purpose of this report is to outline briefly several methods of extending a particular algebraic system, called a field, to a larger field containing this initial field as a proper subset or a subset isomorphic to the initial field.

The first extension this report considers is the transcendental field extension. The field is first extended to its polynomial domain. It is then noted that ordered pairs of the elements of the polynomial domain, with appropriate definitions for operations and equality, form a field containing the original field as a proper subset.

In the second method, the algebraic extension of a field, the field is again extended to a polynomial domain.

This domain is then reduced modulo an irreducible polynomial into a set of residue classes. These residue classes, with definitions for addition, multiplication, and equality, form a field.

In the final extension by valuation, the elements of an ordered field are formed into regular sequences. Here again it is observed that, under appropriate definitions for operations and relations, the set of sequences behave as a field.