FINITE FIELD EXTENSIONS & GALOIS GROUPS

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teachers College

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts in Mathematics

---

by

Verle Edward Harrison

August 1964

GRADUATE COUNCIL APPROVAL

Laurence L. Boyle

DEPARTMENTAL APPROVAL

Marion P. Emerson

ACKNOWLEDGEMENT

I would like to express my appreciation to Dr. Emerson for his help and encouragement, and also to my wife, Barbara, for her willingness to put up with mathematics at dinner.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

Often in elementary algebra, equations are found that have no solution over a given field. This gives rise to at least two questions. First, if we change the field of the equation, will the equation have a solution? Second, if the equation does have a solution, can it be found only by rational operations and extraction of roots? Both of these questions are now answerable by means of modern abstract algebra, especially group and Galois Theory.

I. THE PROBLEM

Statement of the problem. The purpose of this study is (1) to show the development of a root field extension of an irreducible algebraic equation; (2) to define the Galois group of an equation and give some specific examples of Galois groups; (3) to show by using Galois Theory the existence of equations of degree five and higher that are not solvable by radicals and give an example of such an equation.

Limitations. Since there has been such an extensive development of finite groups, fields, and Galois Theory, this paper can deal with only a few aspects of these areas. Only a brief introduction to Galois Theory is given; however, included are numerous examples of field extensions and Galois groups.

Importance of the problem. Field extensions and groups, particularly root field extensions and the associated Galois group, play an

In a letter to a friend written on the eve of his death, Evariste Galois (1811-1832) outlined some of his thoughts in mathematics. This letter contained the basis of what has been called "Galois Theory." He was the first mathematician to give a necessary and sufficient condition for an algebraic equation to be solvable by radicals. One of the basic theorems establishes a relationship between subfields of a field and subgroups of a Galois group.

From the original work of Abel and Galois many mathematicians have enlarged upon the idea of a group until today it is one of the most important abstract mathematical structures. Cauchy (1789-1857) is credited as the founder of the theory of groups of finite order. He proved a theorem previously stated by Galois, but now called Cauchy's Theorem. One of the first persons to treat groups abstractly was Cayley (1821-1895) in a paper in 1854.

In recent years the work of such men as Dickson (1874-1954), who did a great deal of work with Galois Fields, and Moore (1862-1932), who showed all finite fields may be thought of as Galois Fields, show the importance of the ideas stated in the letter written by Galois on the eve of his fatal duel.

III. DEFINITIONS OF TERMS USED

The reader is assumed to be familiar with the ideas usually taught in a course in modern abstract algebra. Below are several definitions found in any standard textbook and are included here to help refresh the memory of the reader.

Algebraic element. A zero of a polynomial with coefficients from a ring is called an algebraic element. Any other element is transcendental.

Automorphism. An isomorphism of a set with itself is called an automorphism.

Basis. A basis of a vector space is a linearly independent subset of the vector space which generates the whole space. A vector space is finite-dimensional if and only if it has a finite basis.

Characteristic of a field. If there is a positive integer n such that na = 0 for every element of field F, then the smallest such integer n is called the characteristic. If no such integer exists, field F is said to have characteristic zero. Note: na means $\sum_{i=1}^{n} a_i$, where for all i, $a_i = a$.

Conjugate. Algebraic elements are conjugates if they are roots of the same irreducible polynomial.

Coset. If H is a subgroup of the group G and a is an element of G, then aH is called a left coset of H. Ha is called a right coset of H. If aH = Ha for all $a \in G$, then H is an invariant subgroup or normal divisor.

Irreducible polynomial. A polynomial which has no zeros in a field F is called an irreducible polynomial over F.

Isomorphism. A 1-1 mapping of an algebraic system onto another system which preserves operations.

Order. The order of a group is the number of elements in the group.

Prime field. A field which has no proper subfields is called a prime field.

The proofs of the following theorems may be found in many textbooks on abstract algebra or group theory and they are therefore omitted here.

Cayley's Theorem. Every abstract group is isomorphic to a permutation group. (4, p. 69)

Gauss' Lemma. The product of any two primitive polynomials is itself primitive. (3, p. 98)

Lagrange's Theorem. If the group G has order n, the order of every subgroup H of G is a divisor of n. (5, p. 188)

Theorem 1.1. A group of prime order has no proper subgroups and is necessarily cyclic. (3, p. 147)

Theorem 1.2. All subgroups of a cyclic group are cyclic. (7, p. 21)

Theorem 1.3. The only prime fields are the field of integers modulo p and the field of rational numbers.

Proof: Since every field is an integral domain, all fields are of either characteristic 0 or characteristic p. Consider a field of characteristic p. The elements of the additive group generated by the unity element e will form a field isomorphic to the field of integers modulo p, using the mapping $ae \longleftrightarrow a_p$, where a is an element of the additive group and a_p is the residue class a of integers modulo p. Hence every field of characteristic p contains a subfield isomorphic to the field of integers modulo p. Now consider a field of characteristic 0. The subgroup generated by the unity element e will be isomorphic to the domain of integers, using the mapping $ae \longleftrightarrow a$, where $a \in I$. The subfield generated by e will contain all quotients ae/be, $b \neq 0$ and hence is isomorphic to the field of rational numbers, using the mapping $ae/be \longleftrightarrow a/b$, $b \neq 0$.

Hence all fields of characteristic 0 contain a subfield isomorphic to the field of rational numbers.

The following is a list of notation that will be used in this thesis:

G	Denotes a group
F	Denotes a field
K	Will always denote an extension field
$F \subseteq K$	F is a subfield of K
$F(a_1, a_2, \ldots)$	The extension of F by the elements a_1, a_2, ...
C	Field of complex numbers
Re	Field of real numbers
R	Field of rational numbers
I	Set of integers
Q/R	Vector space Q over R
(K/F)	Degree of the extension K over F
F[x]	Ring polynomials in x over F
f(x)	Polynomial
$GF(p^n)$	Galois Field of p^n elements

CHAPTER II

FIELDS AND THEIR EXTENSIONS

The purpose of this chapter is to give an introduction to the theory of field extensions, particularly finite field extensions.

Definition 2.1. K is an extension field of F if F is a subfield of K. Notation: $F \subseteq K$.

Consider a set $S = \{a_1, a_2, a_3, \ldots\}$ of elements of K; and let $F(a_1, a_2, \ldots)$ denote a set of elements in K which arises from rational operations with the elements of F and the elements of S. Hence $F(a_1, a_2, \ldots)$ is a field and also the smallest extension of F containing S. (2, p. 13)

Definition 2.2. The field $F(a_1, a_2, a_3, \ldots)$ is said to be formed by the adjunction of the elements of set S.

Definition 2.3. If $K = F(a_1)$, then K is called a simple extension.

Example: If $K = F(u)$, then the elements of K would be of the form $(a_0 + a_1u^1 + a_2u^2 + \ldots)(b_0 + b_1u^1 + b_2u^2 + \ldots)^{-1}$, where $a_i, b_i \in F$ and u is the adjoined element.

We may consider any finite extension as arising from repeated or iterated extensions.

For example: Suppose $K = R(\sqrt{2}, \sqrt{3})$ then it has elements of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$, where $a, b, c, d \in R$, i.e. all rational operations with elements of R and the elements $\sqrt{2}$ and $\sqrt{3}$. Now let $J = R(\sqrt{2})$ and $L = J(\sqrt{3})$

$$a + b\sqrt{2} \in J \qquad a, b, \in R$$

$$c_1 + d_1\sqrt{3} \in L \qquad c_1, d_1, \in J$$

but $c_1 = e + f\sqrt{2}$ and $d_1 = g + n\sqrt{2}$ $e, f, g, h \in R$. Hence substituting for c_1 and d_1

$$(e + f\sqrt{2}) + (g + h)\sqrt{2})\sqrt{3} \in L$$

$$e + f\sqrt{2} + g\sqrt{2} + h\sqrt{2}\sqrt{3} \in L$$

Therefore L = K. In general the simple extension of F by the element u_1 followed by the simple extension of $F(u_1)$ by the element u_2 yields the same field as $F(u_1, u_2)$. Furthermore the order of adjunction is immaterial, i.e. $F(u_1, u_2) = F(u_2, u_1)$. It can be shown by mathematical induction that any finite extension may be obtained by this process of iterated extensions.

Definition 2.4. If the elements of set S are algebraic, then $F(a_1, a_2, a_3, \ldots)$ is called an algebraic extension; otherwise, it is a transcendental extension.

Example: The field of complex numbers C is an algebraic extension of the field of real numbers Re. The elements of C are of the form a + bi where a, b $\in$ Re and i is the adjoined element. Using the above notation this field is also denoted by Re(i). An example of a transcendental field extension of the rational numbers R is $R(\pi)$ with elements $(a_0 + a_1\pi + a_2\pi^2 + \ldots)(b_0 + b_1\pi + b_2\pi^2 + \ldots)^{-1}$, where $a_i, b_i \in R$ and π is the adjoined element. Both of these extensions are simple since they are created by the adjunction of one element.

Theorem 2.1. Any two simple transcendental extensions of the same field are isomorphic.

Proof: Consider the two extensions of field F, F(v) and F(w) where v and w are transcendental. Now F(v) and F(w) are clearly isomorphic under the mapping $v \longleftrightarrow w$, by considering the elements of each field as polynomials in indeterminates v and w respectively.

An extension K of a field F is a vector space, where the elements of F are the scalars and the elements of K are the vectors, since for a, b $\in$ F and A, B $\in$ K we have the following:

$$a(A + B) = aA + aB$$

$$(a + b)A = aA + bA$$

$$a(bA) = (ab)A$$

$$1A = A$$

Hence the extension K of F is a vector space over F and is denoted K/F. The dimension of this vector space is the degree of the extension K over F and is denoted by (K/F). An extension is called finite if its degree is finite.

Theorem 2.2. If $F \subseteq K \subseteq K'$, then $(K'/F) = (K'/K)(K/F)$, where K and K' are finite extensions.

Proof: Let $(K'/F) = n$, $(K'/K) = m$, $(K/F) = q$ and let the basis of K'/K be $v_1, v_2, \ldots v_m$ and the basis of K/F be $w_1, w_2, \ldots w_q$. Now if $t \in K'$ and $r \in K$ they are of the form

$$t = \sum_{i=o}^{m} a_i v_i \qquad r = \sum_{j=o}^{q} b_j w_j \qquad a_i \in K,\ b_j \in F$$

now by substituting for a_i

$$t = \sum_i \left(\sum_j b_{ij} w_j \right) v_i$$

$$t = \sum_i \sum_j b_{ij} (w_j v_i)$$

Hence the independence of the elements of K' depends upon the independence of w_j and v_i. These are linearly independent with respect to F, since if they were not $\sum_i \sum_j b_{ij} w_j v_i = 0$ and since the v_i's are linearly independent with respect to K then $\sum_j b_{ij} w_j = 0$ but the w_j's are linearly independent with respect to F. Therefore mq is the degree of the extension K' of the field F.

Theorem 2.3. An extension K of F is algebraic if and only if the degree of the extension K is finite.

Proof: Let the extension K over F have finite degree n and let $a \in K$. Since the powers $1, a^1, a^2, \ldots, a^n$ are linearly dependent, then there are c_i's, not all zero, such that $\sum_{i=0}^{n} c_i a^i = 0$. Consider the equation $\sum_{i=0}^{n} c_i x^i$. The element a of K is a solution of this equation; hence K is algebraic.

Now assume K is algebraic. Adjoin any algebraic element of degree n. This gives us a finite extension with basis $1, a, \ldots, a^n$. By Theorem 2.2 successive finite extensions always yield finite extensions. Hence K is a finite extension.

We may now use the terms finite algebraic extension, finite extension, and algebraic extension interchangeably.

Definition 2.5. If an extension K is formed by the adjunction of all roots of an equation $f(x) = 0$, then it is a root field (also called splitting field or decomposition field). This means that f(x) must factor into linear factors in K and that $K = F(a_1, a_2, \ldots, a_n)$ where $f(a_i) = 0$. Note: Most of the fields in this paper will be root fields.

Example of a root field extension:

Consider the field of rational numbers and the equation $x^3 - 2 = 0$. The roots are r, wr, w^2r, where $r = \sqrt[3]{2}$ and $w^3 = 1$, then the root field would be $K = F(r, wr, w^2r)$, with elements of the form $a + br + cwr + dw^2r + ewr^2 + fw^2r^2$. Note: This field may be formed other ways also, i.e. K = F(w,r) is exactly the same field.

Theorem 2.4. For every polynomial f(x) of degree n in $F[x]$, there exists a root field.

Proof: Either $f(x)$ is completely reducible into linear factors or it has irreducible factors. In the first case F is the root field; therefore, assume it has irreducible factors. Factor $f(x)$ into these factors. $f(x) = f_1(x)\ f_2(x)\ f_3(x) \ldots f_n(x)$. Now adjoin a root r_1 of $f_1(x)$ to F obtaining $F(r_1)$. Now factor $f(x)$ into irreducible factors over $F(r_1)$ and continue this process. There are at most n steps, since $f(x)$ is of finite degree.

Theorem 2.5. If $r_1, r_2, \ldots, r_n$ are conjugates, then the fields $F(r_1), F(r_2), \ldots, F(r_n)$ are isomorphic. (3, p. 382)

Another classification of extensions follows from the idea of root fields.

Definition 2.6. A field K is called normal over F, if it is algebraic over F and if every irreducible polynomial $f(x)$ in $F[x]$, which has one root in K, factors completely into linear factors in K.

Theorem 2.6. If $K = F(a_1, \ldots, a_n)$ is formed by the adjunction of all roots of a polynomial $f(x)$, then K is normal.

Proof: Let $g(x)$ have a root r in K, but assume $g(x)$ does not factor into linear factors in K. Now extend K to a field $K(r')$ by the adjunction of another root r' of $g(x)$. Since r and r' are conjugate, $F(r) \longleftrightarrow F(r')$, under this isomorphism the elements of F and the coefficients of $f(x)$ remain fixed. By adjoining all roots of $f(x)$ to both $F(r)$ and $F(r')$, we obtain the following: $F(r, a_1, \ldots, a_n) \longleftrightarrow F(r', a_1, \ldots, a_n)$, where a_i is mapped on some a_j. Now r is a rational function of $a_1, a_2, \ldots, a_n$ since r is a root in K, and this relationship is preserved in an isomorphism. Hence r' is also a rational function of $a_1, \ldots, a_n$ and must belong to K. We have a contradiction and therefore K must be normal.

Definition 2.7. If r is a root of an irreducible polynomial f(x) in F[x] which has no multiple roots in K, then r is called separable over K. Likewise f(x) is called separable. If f(x) has multiple roots, then f(x) and the roots are called inseparable. An algebraic extension K over F is separable if all the elements of K are separable over K, and any other extension is inseparable.

Theorem 2.7. Case I. For fields of characteristic zero, all irreducible polynomials in F are separable.

Case II. For fields F of characteristic p, all irreducible polynomials in F are separable, provided f(x) cannot be written as a function of x^p.

Proof: For any polynomial f(x) to have multiple zeros, f(x) and f'(x) must have a linear factor in common. Consider an irreducible polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ then $f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}$. Now since f(x) is irreducible, the greatest common divisor of f(x) and any polynomial of lower degree must be 1. Hence f'(x) = 0. Now if f'(x) = 0 for all values of x, then the coefficients of f'(x) must be zero. Therefore $ia_i = 0$ for all i. If K is of characteristic zero, then the $a_i = 0$ for all $i \neq 0$. Therefore f(x) has no multiple roots in K. Now if K has characteristic p and if $ia_i = 0$ for all i, then $i \equiv 0$ modulo p. Hence if f(x) has multiple roots, all terms must vanish except $a_i x^i$ with $i \equiv 0$. Therefore $f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_n x^{np}$. Conversely, if f(x) is in this form, then f'(x) = 0. Hence we may write $f(x) = g(x^p)$. Note: Usually in forming a root field extension we consider only irreducible polynomials. This theorem is one of the reasons, since it requires the polynomials to be irreducible.

All of the previous work in this paper has been concerned with fields and field extensions in general. The theorems apply to both finite and infinite fields. Now let us direct our attention to finite fields. Perhaps the best way to understand the ideas of field extensions is to actually write out the addition and multiplication tables of some field extension. Unfortunately this is impossible in the case of infinite fields, but it is possible with small finite fields. Before writing out these tables, some theorems about finite fields and their extensions should be proved. Finite fields are often called Galois Fields. First consider a Galois Field K with q elements. Since K cannot have characteristic zero, call it p. Now K has a finite number of elements, hence its basis over the field of integers modulo p is at most n. Let F be this field of integers modulo p. Every element of K must be of the form $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ $a_i \in F$. For each a_i there are p choices possible. Hence there must be p^n elements in K. Therefore the number of elements of a Galois Field is a power of the characteristic p and the exponent denotes the degree of the field extension K. A Galois Field with p^n elements is denoted by $GF(p^n)$. Note: $GF(p^1)$ is another name for the field of integers modulo p.

Theorem 2.8. All Galois Fields with $q = p^n$ elements are isomorphic.

Proof: Omitting the zero element the elements of the Galois Field form an Abelian group under multiplication, of order $q - 1$. Hence $a^{q-1} = 1$, $a \neq 0$. $a^q - a = 0$. Hence all elements satisfy the equation $x^q - x = 0$. Therefore $GF(p^n)$ arises by the adjunction of all roots of $x^q - x = 0$. Hence K is uniquely determined, except for isomorphisms.

This theorem points out an important difference between finite and infinite fields. In finite fields, if they have the same number of elements, then they are isomorphic; however, this is not necessarily true in infinite fields.

Now it is necessary to show that there does exist a finite field with p^n elements.

Theorem 2.9. There exists for all primes p and all integers $n > 0$ a finite field with p^n elements.

Proof: Let f be a field with characteristic p. Now form $K = F(a_1, \ldots, a_q)$ where $q = p^n$ which resolves the polynomial $x^q - x$ into linear factors. Now consider set $s = \{a_1, \ldots, a_q\}$, where a_i is a root of $x^q - x = 0$. This set forms a field since $x^q = x$ and $y^q = y$, and hence $(x - y)^q = x^q - y^q$, and also $(x/y)^q = x^q/y^q$, $y \neq 0$. $x^q - x$ is separable since $f'(x) = qx^{q-1} = 0$ modulo p. Therefore K is a field with p^n elements.

Now having a few basic theorems in hand, consider developing the addition and multiplication tables for several field extensions. First extend the field GF(2) by the roots of the irreducible polynomial $x^2 + x + 1$. Consider the equation $x^2 + x + 1 = 0$ or $x^2 = 1 + x$. Now if j is a root of this equation, then $j^2 = 1 + j$. First write all rational combinations of j and the elements of GF(2). They are of the form $a + bj$, where $a, b \in GF(2)$. These elements are 0, 1, j, 1 + j.

The addition table is straightforward, but let us develop the entries in the multiplication table in detail. First of all a field must be commutative. This means the entries in the table must be symmetric about the main diagonal. Now to consider the table entry by entry.

0 must be the zero element so define $0 \cdot a = 0$ for all $a \in GF(2^2)$. Also 1 must be the multiplication identity, hence $1 \cdot a = a$ for all $a \in GF(2^2)$. This leaves the problem of defining $j \cdot j$, $j(1 + j)$, $(1 + j)(1 + j)$. Using the properties of multiplication, these products are j^2, $j + j^2$, $1 + 2j + j^2$ respectively. Using the identity $j^2 \equiv 1 + j$ replace j^2 in each obtaining $1 + j$, $j + (1 + j)$, $1 + 2j + (1 + j)$. Now adding where possible according to the addition table we obtain $1 + j$, 1, j. The table is completed with these elements since each is an element of $GF(2^2)$.

Below are the addition and multiplication tables for the Galois Field $GF(2^2)$.

+	0	1	j	1+j
0	0	1	j	1+j
1	1	0	1+j	j
j	j	1+j	0	1
1+j	1+j	j	1	0

·	0	1	j	1+j
0	0	0	0	0
1	0	1	j	1+j
j	0	j	1+j	1
1+j	0	1+j	1	j

Notice that by Theorem 2.8 we may arrive at this same field by adjoining all roots of the equation $x^4 - x = 0$ over GF(2). By substituting the values 0, 1, j, 1 + j into this equation, it is easily seen that these are roots and since the equation is fourth degree these are the only roots. Also notice that the element j generates a cyclic group with elements j, j^2, j^3, or by multiplying these out j, 1 + j, 1.

Addition and multiplication tables for the Galois Fields $GF(2^3)$ and $GF(3^2)$ with generating polynomials $x^3 + x + 1$ and $x^2 + 2x + 2$, respectively, are given on pages 16 and 17.

$GF(2^3)$
GENERATING EQUATION $x^3 + x + 1 = 0$
ADDITION TABLE

+	0	1	u	u^2	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$
0	0	1	u	u^2	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$
1	1	0	$1+u$	$1+u^2$	u	$1+u+u^2$	$u+u^2$	u^2
u	u	$1+u$	0	$u+u^2$	1	u^2	$1+u^2$	$1+u+u^2$
u^2	u^2	$1+u^2$	$u+u^2$	0	$1+u+u^2$	u	$1+u$	1
$1+u$	$1+u$	u	1	$1+u+u^2$	0	$1+u^2$	u^2	$u+u^2$
$u+u^2$	$u+u^2$	$1+u+u^2$	u^2	u	$1+u^2$	0	1	$1+u$
$1+u+u^2$	$1+u+u^2$	$u+u^2$	$1+u^2$	$1+u$	u^2	1	0	u
$1+u^2$	$1+u^2$	u^2	$1+u+u^2$	1	$u+u^2$	$1+u$	u	0

$GF(2^3)$
MULTIPLICATION TABLE

•	0	1	u	u^2	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$
0	0	0	0	0	0	0	0	0
1	0	1	u	u^2	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$
u	0	u	u^2	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$	1
u^2	0	u^2	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$	1	u
$1+u$	0	$1+u$	$u+u^2$	$1+u+u^2$	$1+u^2$	1	u	u^2
$u+u^2$	0	$u+u^2$	$1+u+u^2$	$1+u^2$	1	u	u^2	$1+u$
$1+u+u^2$	0	$1+u+u^2$	$1+u^2$	1	u	u^2	$1+u$	$u+u^2$
$1+u^2$	0	$1+u^2$	1	u	u^2	$1+u$	$u+u^2$	$1+u+u^2$

$GF(3^2)$
GENERATING EQUATION $x^2 + 2x + 2 = 0$
ADDITION TABLE

	0	1	2	u	1+u	2+u	1+2u	2+2u	2u
0	0	1	2	u	1+u	2+u	1+2u	2+2u	2u
1	1	2	0	1+u	2+u	u	2+2u	2u	1+2u
2	2	0	1	2+u	u	1+u	2u	1+2u	2+2u
u	u	1+u	2+u	2u	1+2u	2+2u	1	2	0
1+u	1+u	2+u	u	1+2u	2+2u	2u	2	0	1
2+u	2+u	u	1+u	2+2u	2u	1+2u	0	1	2
1+2u	1+2u	2+2u	2u	1	2	0	2+u	u	1+u
2+2u	2+2u	2u	1+2u	2	0	1	u	1+u	2+u
2u	2u	1+2u	2+2u	0	1	2	1+u	2+u	u

$GF(3^2)$
MULTIPLICATION TABLE

	0	1	2	u	1+u	2+u	1+2u	2+2u	2u
0	0	0	0	0	0	0	0	0	0
1	0	1	2	u	1+u	2+u	1+2u	2+2u	2u
2	0	2	1	2u	2+2u	1+2u	2+u	1+u	u
u	0	u	2u	1+u	1+2u	1	2	2+u	2+2u
1+u	0	1+u	2+2u	1+2u	2	u	2u	1	2+u
2+u	0	2+u	1+2u	1	u	2+2u	1+u	2u	2
1+2u	0	1+2u	2+u	2	2u	1+u	2+2u	u	1
2+2u	0	2+2u	1+u	2+u	1	2u	u	2	1+2u
2u	0	2u	u	2+2u	2+u	2	1	1+2u	1+u

Since all extensions of finite field may be generated by a single element, often called a primitive element, consider the conditions under which a field of characteristic 0 may be generated by a primitive element.

Theorem 2.10. Let $F(a_1, a_2, \ldots, a_n)$ be a finite algebraic extension field, and let $a_2, a_3, \ldots, a_k$ be separable elements. $F(a_1, a_2, \ldots, a_n)$ is a simple extension, i.e. $F(a_1, a_2, \ldots, a_n) = F(\theta)$.

Proof: First we prove the theorem for two elements, i.e. that $F(a, b) = F(\theta)$. Let $f(x)$ be the irreducible polynomial for a and $g(x)$ that for b. We take a field $F(a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_h)$ in which $f(x)$ and $g(x)$ factor completely into linear factors, where a_i and b_i are distinct zeros of $f(x)$ and $g(x)$ respectively. Let $a_1 = a$ and $b_1 = b$.

Consider $$a_i + xb_j = a_1 + xb_1$$

$$x = \frac{a_1 - a_i}{b_j - b_1} \qquad b_j \neq b_1$$

Hence if $j \neq 1$, this has at most one root in F for every i and every j. Now if we take c different from all of these roots, i.e.

$$c \neq \frac{a_i - a_1}{b_j - b_1} \qquad \text{for all i and } j \neq 1$$

Let $\theta = a_1 + cb_1$ and by substituting for a_1 and b_1

$$\theta = a + cb$$

Then θ is an element of $F(a, b)$ and is the required primitive element. The element b satisfies the equations $g(b) = 0$ and $f(\theta - cb) = 0$, with coefficients in $F(\theta)$. The polynomials $g(x)$, $f(\theta - cx)$ have only one

root in common, namely b; for the other roots of $g(x)$ are b_j, $j \neq 1$ and since $\Theta - cb_j \neq a_i$

$$f(\Theta - cb_j) \neq 0$$

Hence $g(x)$ and $f(\Theta - cx)$ have only one linear factor $x - b$ in common. The coefficients of this greatest common divisor must lie in $F(\Theta)$, hence b lies in $F(\Theta)$ from $a = \Theta - cb$. The same thing follows for a, therefore $F(a, b) = F(\Theta)$. Hence the theorem is true for $n = 2$.

Let $F(a_1, a_2, \ldots, a_{n-1}) = F(\Theta_1)$,

then $F(a_1, a_2, \ldots, a_{n-1}, a_n) = F(\Theta_1, a_n)$

and since $F(\Theta_1, a_n) = F(\Theta)$

$F(a_1, a_2, \ldots, a_n) = F(\Theta)$

Therefore, by induction every separable finite extension is simple.

CHAPTER III

GALOIS GROUPS

This chapter includes the definition of a Galois group. Galois Theory establishes a relationship between normal field extensions and subgroups of Galois groups. All field extensions in this chapter will be finite separable extensions.

Theorem 3.1. All automorphisms of a field K form a group.

Proof: Consider the set $A = \{ T \mid T \text{ is an automorphism of } K \}$.

Let $a, b \in K$ and $T \in A$, then

$$(a + b)T = aT + bT$$

and $(ab)T = (aT)(bT)$ by the definition of automorphism. The product of any two automorphisms is an automorphism and also the inverse of an automorphism is an automorphism. Hence these automorphisms form a group.

Let K be an extension of F and consider the set B of automorphisms which leave all elements of F fixed or invariant, i.e. if $a \in F$ and $T \in B$, then $aT \in F$ and $aT = a$. These automorphisms form a subgroup of the group of all automorphisms of field K.

For example: Consider $C = Re(i)$, where $a + bi \in C$ and $a, b \in Re$. Only two automorphisms will leave the elements of Re invariant. These are

$$a + bi \longrightarrow a + bi \quad \text{(the identity mapping)}$$

and $$a + bi \longrightarrow a - bi.$$

Call the first automorphism I and the second T, then the multiplication table is

•	I	T
I	I	T
T	T	I

Consider the permutations of i and its conjugate. These permutations are I: (i)(-i) and T': (i -i). The multiplication table is

•	I	T'
I	I	T'
T'	T'	I

Under the correspondence $I \longleftrightarrow I$ and $T \longleftrightarrow T'$, these two groups are isomorphic.

Theorem 3.2. Any automorphism T of a finite extension K over F which leaves all elements of F invariant maps each element r, $r \in K$, into a conjugate rT, $rT \in K$.

Proof: Let $F(x) = x^n + b_{n-1} x^{n-1} + \ldots + b_0$, $b_i \in F$. The automorphism T preserves all rational relations and leaves each element of F fixed (hence each b_i is left fixed).

$$(r^n + b_{n-1}r^{n-1} + \ldots + b_0)T = (rT)^n + b_{n-1}(rT)^{n-1} + \ldots + b_1(rT) + b_0 = 0$$

Hence rT is a root of f(x), and therefore rT is a conjugate of r.

Definition 3.1. Let K be a normal field extension of F and let G be a group of automorphisms which leaves the elements of F invariant. Group G is called the Galois group of K over F; by the Galois group of an

equation $f(x) = 0$, we mean the Galois group of its root field $K = F(r_1, r_2, \ldots, r_n)$.

Hence the above example of an automorphism group is the Galois group of C over Re or the Galois group of the equation $x^2 + 1 = 0$. Since the automorphisms which form a Galois group always leave the elements of F invariant and permute the roots of $f(x) = 0$, the Galois group may be thought of as a permutation group of the roots of an irreducible polynomial over a field F.

Theorem 3.3. The order of a Galois group is the degree of the extension K over F.

Proof: Let the normal field $K = F(r_1, r_2, \ldots, r_n)$ be formed by the adjunction of the roots of an irreducible polynomial of degree n. From Theorem 2.10 $K = F(\theta)$. Now consider the automorphisms which carry $F(\theta)$ into its conjugate fields $F(\theta_i)$ which leave the elements of F invariant. These n automorphisms form the Galois group of K over F, hence if n is the order of the Galois group, $n = (K/F)$.

Since the order of the Galois group depends upon the field which is extended as well as the polynomial, it is necessary to specify both. Consider the polynomial $x^2 - 2$ over the rational numbers. The roots of $x^2 - 2$ are $\sqrt{2}$ and $-\sqrt{2}$. Hence the only automorphisms which permutes the roots are

I: $(\sqrt{2})(-\sqrt{2})$ and U: $(\sqrt{2}\ -\sqrt{2})$. The multiplication table is

·	I	U
I	I	U
U	U	I

Note: This group is isomorphic to the Galois group of the equation $x^2 + 1 = 0$ over R. In general consider an irreducible polynomial $x^2 + ax + b$ over F. The permutations of the roots would be $(c+\sqrt{d})(c-\sqrt{d})$ and $(c+\sqrt{d}\quad c-\sqrt{d})$ where $c = -a$ and $d = a^2 - 4b$. The Galois group of this equation is also isomorphic to the additive group of the integers modulo 2.

Consider the equation $x^3 + x^2 + x + 1 = 0$ over Re. The roots are q, q^2, q^3 where $q^4 = 1$. The Galois group of this equation is a cyclic group of order 3. T: $(q\ q^2\ q^3)$

•	I	T	T^2
I	I	T	T^2
T	T	T^2	I
T^2	T^2	I	T

The roots of $x^4 - 5x^2 + 6 = 0$ over R are $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$.

Let I: identity mapping T: $(\sqrt{3}\ -\sqrt{3})$ U: $(\sqrt{2}\ -\sqrt{2})$ V: $(\sqrt{2}\ -\sqrt{2})(\sqrt{3}\ -\sqrt{3})$

•	I	T	U	V
I	I	T	U	V
T	T	I	V	U
U	U	V	I	T
V	V	U	T	I

Now consider the equation $x^3 - 2 = 0$ over R. From the example on page 10 the basis consists of 6 elements and hence the order of Galois group is 6. Since conjugates map onto conjugates, then the mappings must be a_1: $(r)(wr)(w^2r)$ a_2: $(r\ w^2r)$ a_3: $(r\ wr)$

a_4: $(wr\ w^2r)$ a_5: $(r\ w^2r\ wr)$ a_6: $(r\ wr\ w^2r)$

The multiplication table for this group is

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_5	a_6	a_3	a_4
a_3	a_3	a_6	a_1	a_5	a_4	a_2
a_4	a_4	a_5	a_6	a_1	a_2	a_3
a_5	a_5	a_4	a_2	a_3	a_6	a_1
a_6	a_6	a_3	a_4	a_2	a_1	a_5

$x^4 - 2 = 0$ over Re. I: $(r)(i)$ T: $(r\ ir)(i)$ T^2: $(r\ -r)(i)$ T^3: $(r\ -ir)(i)$ U: $(r)(i\ -i)$ V: $(r\ ir)(i\ -i)$ W: $(r\ -r)(i\ -i)$ S: $(r\ -ir)(i\ -i)$ The roots are r, -r, ir, -ir, where $r^4 = 2$.

	I	T	T^2	T^3	U	V	W	S
I	I	T	T^2	T^3	U	V	W	S
T	T	T^2	T^3	I	S	W	U	V
T^2	T^2	T^3	I	T	V	U	S	W
T^3	T^3	I	T	T^2	W	S	U	V
U	U	W	V	U	I	T^2	T	T^3
V	V	S	U	W	T^2	I	T^3	T
W	W	V	S	U	T^3	T	I	T^2
S	S	U	W	V	T	T^3	T^2	I

All of the above groups are groups of extensions over infinite fields. Consider an n^{th} degree irreducible polynomial over GF(p). The extension field is $GF(p^n)$ and the Galois group is of order n. It is formed by the powers of the mapping T: $a \longleftrightarrow a^p$. Hence the elements of the group are $T, T^2, \ldots, T^n$ where $T^n = 1$ since $(a^p)^n = 1$. Hence the Galois group of $GF(p^n)$ over GF(p) is a cyclic group of order n.

CHAPTER IV

SOLVABILITY OF ALGEBRAIC EQUATIONS

This chapter establishes a relationship between subfields of root field extensions and subgroups of Galois groups. By the use of this relationship questions involving subfields may be answered by using group theory. In particular, the question of finding roots of an equation by radicals is answered.

In the following theorems, G is a Galois group and K is the corresponding root field.

Theorem 4.1. For every intermediate field F', $F \subseteq F' \subseteq K$, there is a subgroup g of G; namely, the set of automorphisms in G which leave each element of F' fixed.

Proof: Consider the extension K over F' and let g' be the corresponding Galois group. All automorphisms of g leave each element of F' fixed. Hence g is the required subgroup of G.

Theorem 4.2. Every intermediate field F' is uniquely determined by the subgroup g of G.

Proof: Consider the images of the elements of K under the automorphisms of g. The only elements left invariant are the elements of F'. Hence F' is uniquely determined.

Theorem 4.3. For every subgroup g of G, there is a field F' which is the set of elements left invariant by the automorphisms of g.

Proof: Let $K = F(\theta)$ and g be a given subgroup of G with order m. F' is the subfield determined by g, namely the elements of K left invariant by the automorphisms of g. F' is a field since if a and b are left

invariant under the automorphisms of g so is a + b, a - b, ab, and a/b, $b \neq 0$. Also $F \subseteq F' \subseteq K$ since g is a subgroup of G. The Galois group of K over F', call it g' and its order m', contains g as a subgroup since all automorphisms of g leave the elements of F' invariant. Hence $m' \geq m$ and $(K/F') \geq m$, but the degree of the extension K over F' cannot be greater than the order of its Galois group. Therefore $g' = g$.

Theorem 4.4. The order of g is the degree of K over F', i.e. if a is the order of g then $a = (K/F')$, and the index of g in G is the degree of F' over F, i.e. if b is the index of g in G, then $b = (F'/F)$.

Proof: This follows from Theorem 3.3 and Theorem 4.3.

The above four theorems are often included as one theorem and called the Fundamental Theorem of Galois Theory. These theorems state that there is a one-to-one correspondence between the intermediate fields of a normal extension and the subgroups of the Galois group. One immediate consequence of these theorems is that there are a finite number of intermediate fields between F and K. This follows from the finite number of subgroups of a finite group.

Definition 4.1. A group G is solvable if it contains a sequence of subgroups $G = G_0 \supset G_1 \supset \ldots \supset G_n = 1$, where each is a normal subgroup of the preceding and G_{i-1}/G_i is abelian.

Theorem 4.5. The symmetric group S_n, $n > 4$, is not solvable. (3, p. 438)

Definition 4.2. The extension field K over F is called an extension by radicals if there exists intermediate fields F_i, $F \subset F_1 \subset \ldots \subset F_h = K$, where $F_i = F_{i-1}(u_i)$ and u_i is a root of an equation of the form $x^{n_i} - a_i = 0$, $a_i \in F_{i-1}$.

Definition 4.3. A polynomial f(x) over F is solvable by radicals if its root field lies in an extension by radicals.

Theorem 4.6. The polynomial f(x) over F is solvable by radicals if and only if its Galois group G is solvable.

Proof: Assume f(x) is solvable and call K the root field for f(x), then there is a sequence of fields $F \subset F_1 \subset \ldots \subset F_r$ which contains K. Each field F_i is an extension of F_{i-1} by an n^{th} root of unity. Let H be the Galois group of F_r over F. To the sequence of field above there corresponds a sequence of groups $H = H_0 \supset H_1 \supset \ldots \supset H_r = 1$, where each H_{i-1}/H_i is a cyclic group, since they are the Galois groups which corresponds to an extension field formed by the adjunction of the n^{th} roots of unity. Hence H is solvable. G is a normal subgroup of H, and H/G is the group of F'/F, and is therefore the group of the polynomial f(x). But H/G is a homomorph of the solvable group G and hence is itself solvable. (2, p. 61)

Assume group G of f(x) is solvable and F' be the root field. Let $G = G_0 \supset G_1 \supset \ldots \supset G_r = 1$ be a sequence of groups, where G_{i-1}/G_i is an abelian group. Call the corresponding fields $F \subset F_1 \subset \ldots \subset F_r$, where F_i is a normal extension of F_{i-1} and formed by the adjunction of n^{th} roots of unity. Hence F_i is a root field of a polynomial of the form $(x^n - a_1)(x^n - a_2) \ldots (x^n - a_h)$ so that by forming the successive root fields of $x^n - a_k$, F_i is an extension of F_{i-1} by radicals from which it follows K is an extension by radicals. (2, p. 61)

By Theorem 4.6 and 4.5 a polynomial which has a Galois group S_5 is not solvable. Consider a polynomial F(x) which is decomposed modulo p. $f(x) \equiv R_1(x)\ R_2(x) \ldots R_h(x)$, where R_i is irreducible modulo p and let the

degree of R_i be j_i. As soon as the degree j_i is known, the permutations of the roots are known. Namely the permutation consists of cycles j_i, i = 1, 2, ..., h. The Galois group G will contain these j_i cycles. (7, p. 191)

Example: Consider the equation $x^5 - x - 1 = 0$. Decompose it into $(x^2 + x + 1)(x^3 + x^2 + 1)$ modulo 2 and into $x^5 - x - 1$ modulo 3, hence the group contains a cycle of five elements, and a product of a transposition and a three cycle. These elements yield the symmetric group S_5 and hence $x^5 - x - 1$ is not solvable by radicals. (7, p. 191)

Consider the polynomial $x^5 - px - p$ (or $x^5 + px + p$), where p is a prime. Decompose it into $(x^2 + x + 1)(x^3 + x^2 + 1)$ modulo 2 and into $x^5 - px - p$ modulo p. This also contains cycles (12345) and (12)(345) and hence is not solvable.

The above examples show equations of the fifth degree which are not solvable. Now to construct a polynomial of n^{th} degree with a symmetric group, choose a polynomial $f_1(x)$ of degree n, irreducible modulo 2, then a polynomial $f_2(x)$ which resolves modulo 3 into an irreducible factor of degree n - 1 and a linear factor, and then a polynomial $f_3(x)$ which resolves into a quadratic and into one or two odd irreducible factors modulo 5. It is possible to pick all of these polynomials since there are irreducible polynomial of degree m over GF(p). Now pick $f(x) = 15 f_1(x) + 10 f_2(x) + 6 f_3(x)$. (7, p. 192) The Galois group of $f(x)$ is S_n and hence is not solvable for $n > 4$.

CHAPTER V

SUMMARY

This thesis presents examples of finite field extensions and many theorems about these extensions in Chapter I. Chapter II develops the idea of the Galois group of an equation and also includes several examples of Galois groups. In the third chapter a relationship is shown between the subgroups of a Galois group and subfields of normal field extensions. The fourth chapter uses the relationship developed in chapter three to show the existence of equations which are not solvable by radicals.

One notable possibility for further study is for the construction of an equation that has its Galois group isomorphic to a given group.

BIBLIOGRAPHY

BIBLIOGRAPHY

A. BOOKS

1. Albert, A. Adrian. Fundamental Concepts of Higher Algebra. Chicago: The University of Chicago Press, 1956.

2. Artin, Dr. Emil. Galois Theory. Notre Dame, Indiana: University of Notre Dame, 1942.

3. Birkhoff, Garrett, and Saunders MacLane. A Survey of Modern Algebra. New York: The Macmillan Company, 1941.

4. MacDuffee, Cyrus Colton. An Introduction to Abstract Algebra. New York: John Wiley and Sons, Inc., 1940.

5. McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960.

6. Postnikov, M.M. Fundamentals of Galois' Theory. Delhi, India: Hindustan Publishing Corporation, 1961.

7. van der Waerden, B.L. Modern Algebra. Vol. 1. (Published by authority of Attorney General of the U.S.) New York: Frederick Ungar Publishing Company, 1949. Translated by Fred Blum.

APPENDIX

Theorem A.1. Construct a polynomial which is inseparable.

Proof: Let F be a field with characteristic p, and w an indeterminate. Now consider the field $K = F(w)$ and the polynomial $x^p - w = 0$ in $K[x]$. Now $x^p - w = 0$ is irreducible by Gauss' Lemma. Consider the algebraic extension $K(w^{1/p})$. $x^p - w = 0$ is now reducible in $K(w^{1/p})$ since $(w^{1/p})^p - w = 0$. Also since F is of characteristic p, $z^p - x = (z - x^{1/p})^p$ and hence $(z - x^{1/p})^p = 0$. Therefore this polynomial has only one root in $K(w^{1/p})$, but it is of degree p. Hence it is inseparable.

Note: This is one of the few ways to develop an inseparable polynomial and hence most polynomials are separable.