MASTIN, MILLICENT GAY. Classical Galois Theory. (1972)
Directed by Dr. Andrew F. Long. Pp. 48.

Let K be an extension of a field F of characteristic zero and let G be the group of automorphisms of K. A characterization of the subgroups of G and the corresponding fixed fields is developed, and it is shown that there is a one-to-one correspondence between closed subfields of K and closed subgroups of G. It is then shown that K is a normal extension of F if and only if K is the splitting field of some polynomial p(x) over F.

Using these results, it is shown in the Fundamental Theorem of Galois Theory that there is a one-to-one correspondence between subfields of K, the splitting field of p(x), which contain F onto the subgroups of the group of automorphisms of K relative to F. These results are then applied to a fourth degree polynomial over the rational numbers.

CLASSICAL GALOIS THEORY

by

Millicent Gay Mastin

A Thesis Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
August, 1972

Approved by

Andrew E. Long, Jr.
Thesis Adviser

APPROVAL SHEET

This thesis has been approved by the following committee of the Faculty of the Graduate School at the University of North Carolina at Greensboro.

Thesis Adviser Andrew Z. Long, Jr.

Oral Examination Committee Members Robert L. Burkhardt

E.E. Posey

Karl Ray Gentry

August 8, 1972
Date of Examination

ACKNOWLEDGMENT

The author wishes to express her appreciation to Dr. Andrew F. Long for his patience and assistance during the writing of this thesis.

TABLE OF CONTENTS

Page

INTRODUCTION. v

CHAPTER I: PRELIMINARIES 1

CHAPTER II: FIELD EXTENSIONS 8

CHAPTER III: AUTOMORPHISMS AND FIXED FIELDS. 23

CHAPTER IV: NORMAL EXTENSIONS. 30

CHAPTER V: FUNDAMENTAL THEOREM OF GALOIS THEORY. 39

SUMMARY 47

BIBLIOGRAPHY. 48

INTRODUCTION

The purpose of this thesis is to examine the correspondence between groups of automorphsims and fields and to prove the Fundamental Theorem of Galois Theory. The fields under consideration are infinite.

Chapter I is devoted to the basic definitions and theorems needed throughout the paper. It has been assumed that the reader has a knowledge of the basic properties of groups, rings, integral domains, fields, and isomorphisms. Standard theorems have been stated without proofs but with a reference to a proof.

In Chapter II, the basic properties of field extensions, considered as vector spaces, are investigated. Several theorems which characterize splitting fields, simple extensions, and separable extensions are proved. It is then shown that a finite, separable extension is a simple extension.

The concepts of automorphism groups and fixed fields are introduced in Chapter III. This discussion concludes by showing that there is a one-to-one correspondence between closed subfields and closed subgroups of the group of automorphisms of a field.

Chapter IV is devoted to a discussion which characterizes normal extensions. The chapter concludes by establishing an important relationship between normal extensions and splitting fields.

The results of the preceding chapters are then used in Chapter V to prove the Fundamental Theorem.

CHAPTER I

PRELIMINARIES

The following basic definitions and theorems will be used throughout the paper.

1.1 DEFINITION. Let F be a field. If there exists a positive integer p such that $pa = 0$ for each a in F, the smallest such p is called the *characteristic* of F. If no such positive integer exists, F is said to have *characteristic zero*.

1.2 THEOREM. The characteristic of a field F is either zero or a prime.

Proof: Let F be a field and $0 \neq a \in F$. If there is no positive integer p such that $pa = 0$, then by definition, F is of characteristic zero.

Suppose the characteristic of F is p, where p is not a prime. Then there are positive integers $r < p$ and $s < p$ such that $p = rs$. Now $pa = (rs)a = r(sa) = 0$. By the properties of an integral domain, $r = 0$ or $sa = 0$. Since $r > 0$, $sa = 0$. But $s < p$ and p is the smallest positive integer such that $pa = 0$. Hence $sa \neq 0$. Thus p must be a prime.

1.3 DEFINITION. Let F be a field. An isomorphism from F onto itself is called an *automorphism*.

1.4 THEOREM. The set of automorphisms for a field F form a group under composition of mappings.

Proof: Let ϕ, σ, θ be automorphisms of F. Let a and b be in F. By definition of composition $\phi(\sigma(a)) = \phi\sigma(a)$. Since ϕ and σ are one-to-one and onto, then $\phi\sigma$ is one-to-one and onto. Now

$$\begin{aligned} \phi\sigma(a + b) &= \phi(\sigma(a + b)) \\ &= \phi(\sigma(a) + \sigma(b)) \\ &= \phi(\sigma(a)) + \phi(\sigma(b)) \\ &= \phi\sigma(a) + \phi\sigma(b) \end{aligned}$$

and $\phi\sigma(ab) = \phi(\sigma(ab)) = \phi(\sigma(a)\sigma(b)) = \phi(\sigma(a))\phi(\sigma(b)) = \phi\sigma(a)\phi\sigma(b)$. Hence $\phi\sigma$ is an automorphism of F, and F is closed under composition of mappings.

Associativity follows from the definition of composition. Let I: $a \to a$. Then $\phi I(a) = \phi(I(a)) = \phi(a)$. Thus I is the identity automorphism since $I(a + b) = a + b = I(a) + I(b)$ and $I(ab) = ab = I(a)I(b)$.

Now, let ϕ^{-1}: $\phi(a) \to a$. Since ϕ is one-to-one and onto, ϕ^{-1} exists and is one-to-one and onto. Then $\phi^{-1}\phi(a) = a = I(a)$. Hence ϕ^{-1} is the inverse automorphism since

$$\begin{aligned} \phi^{-1}(\phi(a) + \phi(b)) &= \phi^{-1}(\phi(a + b)) \\ &= a + b \\ &= \phi^{-1}\phi(a) + \phi^{-1}\phi(b) \end{aligned}$$

and $\phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}\phi(a)\phi^{-1}\phi(b)$. Thus the automorphisms of F form a group under composition of mappings.

1.5 THEOREM. Any field of characteristic zero has a subfield isomorphic to the rationals $\mathcal{Q}$.

Proof: Let F be a field of characteristic zero. Let $a \in F$. Then there is no positive integer p such that $pa = 0$. Let e be the multiplicative identity in F. Then e, $2e$, . . . , ne, . . . are all distinct elements of F.

Let 0 be the additive identity in F. By the field properties $-e$, $-2e$, . . . , $-ne$, . . . are in F. Let r, $s \in \mathcal{Z}$, the integers. Then re, $se \in F$, so $re/se \in F$. Let K be the subset of F with elements re/se, where r, $s \in \mathcal{Z}$, $s \neq 0$. Then K is a subfield of F and K is isomorphic to $\mathcal{Q}$. For let re/se, $ae/be \in K$, where r, s, a, $b \in \mathcal{Z}$, s, $b \neq 0$. Then

$$\begin{aligned} re/se - ae/be &= ((re)(be) -(ae)(se))/((se)(be)) \\ &= ((rb)e - (as)e)/((sb)e) \\ &= ((rb - as)e)/((sb)e) \in K. \end{aligned}$$

Now let $a \neq 0$. Then $(re/se)(ae/be)^{-1} = (re/se)(be/ae) = (rb)e/(sa)e$ is in K. Hence K is a subfield of F. Define a mapping ϕ from K into $\mathcal{Q}$ by $\phi(re/se) = r/s$ for all $r/s \in \mathcal{Q}$, where r, $s \in \mathcal{Z}$, $s \neq 0$. Assume $\phi(re/se) = \phi(ae/be)$. Then $r/s = \phi(re/se) = \phi(ae/be) = a/b$, and hence ϕ is one-to-one. By definition of ϕ, ϕ is onto. Finally ϕ is a homomorphism since

$$\begin{aligned} \phi(re/se + ae/be) &= \phi((rb + as)e/(sb)e) \\ &= (rb + as)/(sb) \\ &= r/s + a/b \\ &= \phi(re/se) + \phi(ae/be) \end{aligned}$$

and $\phi((re/se)(ae/be)) = \phi((ra)e/(sb)e) = ra/sb = \phi(re/se)\phi(ae/be)$. Thus K is isomorphic to $\mathcal{Q}$.

1.6 THEOREM. A system of m linear homogeneous equations in n unknowns, where $m < n$, always has a nontrivial solution.

Proof: Consider the system of homogeneous equations

$$\begin{array}{l} L_1 = a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ L_2 = a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \quad \vdots \\ L_m = a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{array}$$

Let $n = 1$. Then $m = 0$. Since there are no equations, there are no restrictions on the unknowns. Then arbitrarily set each x_j equal to one.

Assume the theorem is true for all systems of k equations for $k < m$. If all $a_{ik} = 0$, then the theorem holds for $k = n$. Suppose there is at least one $a_{ik} \neq 0$. Without loss of generality, assume $a_{11} \neq 0$, and it is then possible to multiply by a_{11}^{-1}. Now eliminate x_1 from the remaining $m - 1$ equations. Thus the system becomes

$$\begin{array}{l} L_1 = 0 \\ L_2 - a_{21}a_{11}^{-1}L_1 = 0 \\ \quad \vdots \\ L_m - a_{m1}a_{11}^{-1}L_1 = 0 \end{array}$$

Then there is a nontrivial solution to the original system if there is a nontrivial solution to the new system. The system of equations $L_2, \ldots, L_m$ is a system of $m - 1$ equations in $n - 1$ unknowns. By the induction hypothesis, this system has a nontrivial solution, $x_2, \ldots, x_n$, that is, there exist $n - 1$ unknowns, not all zero, such that $L_2 - a_{21}a_{11}^{-1}L_1 = \ldots = L_m - a_{m1}a_{11}^{-1}L_1 = 0$. But $L_1 = 0$ and $a_{11} \neq 0$. Hence there exists $x_1, \ldots, x_n$ not all zero such that $L_1 = \ldots = L_m = 0$.

<u>1.7 THEOREM</u>. Let K be a field and ϕ_i for $i = 1, \ldots, n$ be distinct automorphisms of K. Then it is impossible to find elements a_i for $i = 1, \ldots, n$, not all zero, in K such that

$$a_1\phi_1(u) + \ldots + a_n\phi_n(u) = 0$$

for all $u \in K$.

<u>Proof</u>: Let $u \in K$. Suppose there exist $a_1, \ldots, a_n$ in K, not all zero, such that $a_1\phi_1(u) + \ldots + a_n\phi_n(u) = 0$. Then eliminating the zero terms and renumbering the remaining terms, the expression becomes

$$(1) \quad a_1\phi_1(u) + \ldots + a_m\phi_m(u) = 0$$

where all $a_i = 0$. Suppose $m = 1$. Then $a_1\phi_1(u) = 0$, and hence $a_1 = 0$. But this is a contradiction to the choice of the a_i in (1). Thus $m > 1$. Since the automorphisms are all distinct, there is $c \in K$ such that $\phi_1(c) \neq \phi_m(c)$. Also, $cu \in K$ for all $u \in K$. Thus cu must satisfy (1), that is,

$$(2) \quad a_1\phi_1(cu) + \ldots + a_m\phi_m(cu) = 0.$$

Now multiply (1) by $\phi_1(c)$ and subtract the result from (2). Then

$$a_1\phi_1(u)\phi_1(c) - a_1\phi_1(u)\phi_1(c) + \ldots + a_m\phi_m(u)\phi_m(c) - a_m\phi_m(u)\phi_1(c)$$
$$= a_2\phi_2(u)(\phi_2(c) - \phi_1(c)) + \ldots a_m\phi_m(u)(\phi_m(c) - \phi_1(c)).$$

Now $a_i(\phi_i(c) - \phi_1(c))$ is in K for $i = 1, \ldots, m$ and $a_m(\phi_m(c) - \phi_1(c)) \neq 0$ since $a_m \neq 0$ and $\phi_m(c) \neq \phi_1(c)$. But then the equation above has fewer terms than (1), which contradicts the choice of (1) as the minimal relation. Hence there exist no such a_i in K.

1.8 DEFINITION. The *ring of polynomials* in x over a field F, denoted $F[x]$, is the set of all symbols $a_0 + a_1x + \ldots + a_nx^n$, where n is a nonnegative integer and $a_i \in F$ for $i = 0, \ldots, n$, with the usual addition and multiplication.

Now let $F_1 = F[x_1]$, $F_2 = F_1[x_2]$, the polynomial ring in x_2 over $F_1, \ldots, F_n = F_{n-1}[x_n]$, the polynomial ring in x_n over F_{n-1}. Then F_n is a ring called the *ring of polynomials* in $x_1, \ldots, x_n$ over F, and is denoted $F[x_1, \ldots, x_n]$.

1.9 DEFINITION. Let F be a field and $F[x_1, \ldots, x_n]$ be the ring of polynomials in n variables $x_1, \ldots, x_n$ over F. Then the set of all quotients of polynomials in $F[x_1, \ldots, x_n]$ is called the set of *rational functions* in $x_1, \ldots, x_n$ over F, and is denoted by $F(x_1, \ldots, x_n)$.

1.10 THEOREM. Let F be a field. Then the set of rational functions in $x_1, \ldots, x_n$ over F is a field.

Proof: Let $F(x_1, \ldots, x_n)$ be the set of rational functions in $x_1, \ldots, x_n$ over F. Since F is a field, it is an integral domain. Hence by the properties of integral domain, $F[x_1, \ldots, x_n]$ is an integral domain. Then it is possible to construct the field of quotients of $F[x_1, \ldots, x_n]$. Clearly, the elements of $F[x_1, \ldots, x_n]$ are polynomials in $x_1, \ldots, x_n$ over F. Then the field of quotients of polynomials in $F[x_1, \ldots, x_n]$ is precisely the set of rational functions in $x_1, \ldots, x_n$ over F. Hence $F(x_1, \ldots, x_n)$ is a field.

1.11 DEFINITION. A polynomial $p(x)$ over a field F is said to be irreducible over F if whenever $p(x) = s(x)t(x)$, where $s(x)$, $t(x)$ are in $F[x]$, then one of $s(x)$ or $t(x)$ has degree zero.

1.12 DEFINITION. Let F be a field. If $p(x) = a_n x^n + \ldots + a_1 x + a_0$ in $F[x]$, then the derivative of $p(x)$, denoted by $p'(x)$, is the polynomial $p'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$ in $F[x]$.

1.13 DEFINITION. Let A be the finite set $\{1, \ldots, n\}$. Then the group consisting of the $n!$ possible permutations of A is called the symmetric group on n variables and is denoted by S_n.

1.14 FIRST ISOMORPHISM THEOREM. Let ϕ be a homomorphism from a group G onto a group H with kernel K. Then G/K is isomorphic to H.

Proof: [5]

CHAPTER II

FIELD EXTENSIONS

2.1 DEFINITION. Let F be a field. Then K is an extension of F if F is a subfield of K.

2.2 LEMMA. Let F be a field and K be an extension of F. Then under the field operations of K, K is a vector space over F.

Proof: Since K is a field, clearly K forms an abelian group under addition. Let $\alpha, \beta \in F$ and $v, w \in K$. Since $F \subset K$, then $\alpha v \in K$, $\alpha(v + w) = \alpha v + \alpha w$, $(\alpha + \beta)v = \alpha v + \beta v$, and $(\alpha\beta)v = \alpha(\beta v)$. Hence K is a vector space over F.

2.3 DEFINITION. Let K be an extension of a field F. The degree of K over F is the dimension of K as a vector space over F, and is denoted $[K:F]$.

2.4 DEFINITION. If $[K:F]$ is finite, then K is a finite extension of F.

2.5 THEOREM. Let K, L, M be fields such that $K \subset L \subset M$. Then $[M:K]$ is finite if and only if both $[M:L]$ and $[L:K]$ are finite. In this case $[M:K] = [M:L][L:K]$.

Proof: Suppose $[M:K]$ is finite. Since $L \subset M$, $[L:K]$ must also be finite. Since $K \subset L$, any finite basis that spans M over K must also span M over L, and hence some subset of a basis for M

over K will be a basis for M over L. Thus [M:L] must also be finite.

Suppose [M:L] = m and [L:K] = n. Let u_i for i = 1, . . . , m be a basis of M over L. Let v_j for j = 1, . . . , n be a basis of L over K. Then the mn elements of the form $u_i v_j$ for i = 1, . . . , m and j = 1, . . . , n form a basis for M over K.

Let $x \in M$. Then $x = \sum_{i=1}^{m} \alpha_i u_i$ where $\alpha_i \in L$. Similarly $\alpha_i = \sum_{j=1}^{n} \beta_{ij} v_j$ where $\beta_{ij} \in K$. Thus

$$x = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} v_j \right) u_i = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} u_i v_j .$$

Thus the $u_i v_j$ span M.

Now suppose $\sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} u_i v_j = 0$ for $\beta_{ij} \in K$. Then

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} v_j \right) u_i = \sum_{i=1}^{m} \alpha_i u_i = 0.$$

But the u_i are linearly independent over L. Hence $\alpha_i = 0$ for all i = 1, . . . , m. Thus each $\sum_{j=1}^{n} \beta_{ij} v_j = 0$. But the v_j are linearly independent over K, so each $\beta_{ij} = 0$. Thus the $u_i v_j$ are linearly independent over K, and [M:K] = [M:L][L:K].

2.6 DEFINITION. Let K be an extension of a field F and $u \in K$. Then u is said to be algebraic over F if there exists a polynomial $p(x) \in F[x]$, with coefficients, not all zero, such that $p(u) = 0$.

2.7 DEFINITION. Let K be an extension of a field F. Then K is said to be algebraic over F if every element of K is algebraic over F.

2.8 DEFINITION. Let K be an extension of a field F and u be in K. Then $F(u)$ denotes the intersection of all subfields of K containing both F and u, and $F(u)$ is known as the field obtained by adjoining u to F.

2.9 THEOREM. Let K be an extension of a field F and let $u \in K$. Then $F(u)$ is the smallest subfield of K containing both F and u.

Proof: Let M_i, $i \in I$, be the subfields of K which contain both F and u. Then $F(u) = \cap M_i$. It is necessary to show only that the intersection of fields is a field. Let a, $b \in \cap M_i$. Then a, $b \in M_i$ for all $i \in I$. But since each M_i is a field, $a - b \in M_i$ and $ab^{-1} \in M_i$. Thus $a - b \in \cap M_i$ and $ab^{-1} \in \cap M_i$. So $F(u)$ is a subfield of K.

Now suppose there is a field L containing F and u such that L is a proper subfield of $F(u)$. Then $L \subset \cap M_i$. Since L contains F and u, $L = M_k$ for some $k \in I$. But $\cap M_i \subset M_k = L$. Hence $F(u)$ must be the smallest subfield containing both F and u.

2.10 EXAMPLE. Let $u = \sqrt{5}$. Show $\mathcal{Q}(u) = \{a + bu \mid a, b \in \mathcal{Q}\}$ is a field. Let $a + bu$, $c + du \in \mathcal{Q}(u)$. Then $(a + bu) - (c + du) = (a - c) + (b - d)u$, which is in $\mathcal{Q}(u)$ since $(a - c)$, $(b - d) \in \mathcal{Q}$. Assume $(c + du) \neq 0$. Then

$$
\begin{aligned}
(a + bu)(c + du)^{-1} &= (a + bu)/(c + du) \\
&= ((a + bu)(c - du))/((c + du)(c - du)) \\
&= (ac + (bc - ad)u - 5bd)/(c^2 - 5d^2) \\
&= (ac - 5bd)/(c^2 - 5d^2) + ((bc - ad)u)/(c^2 - 5d^2)
\end{aligned}
$$

These conditions suffice to show that $\mathcal{Q}(u)$ is a subfield of the real numbers.

2.11 THEOREM. Let K be an extension of a field F, $u \in K$, and suppose u is algebraic over F. Let $p(x)$ be a monic polynomial in $F[x]$ of least degree such that $p(u) = 0$, and let this minimal degree be n. Then

(1) $p(x)$ is unique

(2) $p(x)$ is irreducible over F

(3) $1, u, \ldots, u^{n-1}$ form a vector space basis of $F(u)$ over F.

(4) $[F(u):F] = n$

(5) A polynomial $q(x) \in F[x]$ satisfies $q(u) = 0$ if and only if $q(x)$ is a multiple of $p(x)$.

Proof: (1) Suppose $f(x)$ is another monic polynomial of degree n such that $f(u) = 0$. Then

$$
\begin{aligned}
p(x) - f(x) &= \sum_{i=0}^{n} b_i x^i - \sum_{i=0}^{n} c_i x^i \\
&= \sum_{i=0}^{n-1} (b_i - c_i) x^i
\end{aligned}
$$

where b_i, $c_i \in F$ and $b_0 = c_0 = 1$. Then $q(x) = p(x) - f(x)$ is a polynomial of degree less than n, and $q(u) = p(u) - f(u) = 0$. If

$q(x) \neq 0$, this contradicts the fact that n is the minimal degree. Hence $q(x) = p(x) - f(x) = 0$ and $p(x) = f(x)$.

(2) Let $s(x)$, $t(x) \in F[x]$, and $p(x) = s(x)t(x)$. Suppose $p(x)$ is not irreducible. Then neither $s(x)$ nor $t(x)$ is of degree zero, and $s(x)$ and $t(x)$ must both be of degree less than n. But $p(u) = s(u)t(u) = 0$ implies $s(u) = 0$ or $t(u) = 0$ by integral domain properties. Then there is a polynomial of degree less than n which satisfies the conditions. This contradicts the minimal choice of $p(x)$, and hence $p(x)$ is irreducible.

(3) Suppose $1, u, \ldots, u^{n-1}$ are linearly dependent over F. Then there is a polynomial $q(x) \in F[x]$ of degree $k < n$ such that $q(x) = \sum_{i=0}^{k} b_i x^i = 0$, where $b_i \in F$, and not all $b_i = 0$. Then $q(u) = 0$. But this contradicts the choice of n as the minimal degree. Hence $1, u, \ldots, u^{n-1}$ must be linearly independent.

Let T be a subspace of $F(u)$ which is spanned by $1, u, \ldots, u^{n-1}$. Then show T is a field. Let $s, t \in T$. Let $s = s(u)$ and $t = t(u)$, where $s(u)$, $t(u)$ are nonzero polynomials of degree less than n such that $s(u) = \sum_{i=0}^{n-1} \alpha_i u^i$, where $\alpha_i \in F$, and $t(u) = \sum_{i=0}^{n-1} \beta_i u^i$, where $\beta_i \in F$. Then

$$s(u) - t(u) = \sum_{i=0}^{n-1} (\alpha_i - \beta_i)u^i$$

and each $(\alpha_i - \beta_i) \in T$.

Now let $k = n - 1$. Every power of u through $n - 1$ is in T since T is spanned by $1, u, \ldots, u^{n-1}$. Suppose $u^{k-1} \in T$, and show $u^k \in T$. Now,

$$u^k = u(u^{k-1}) = u(\sum_{i=0}^{n-1} \alpha_i u^i) = \sum_{i=0}^{n-1} \alpha_i u^{i+1}$$

where $\alpha_i \in F$. By the minimal polynomial $p(x)$, $p(u) = u^n + \sum_{i=0}^{n-1} b_i u^i$ where $b_i \in F$. Thus $u^n = - \sum_{i=0}^{n-1} b_i u^i$, and u^n can therefore be expressed as a linear combination of 1, $u, \ldots, u^{n-1}$. Hence u^k is a linear combination of 1, $u, \ldots, u^{n-1}$, and by induction $u^k \in T$. Since polynomials $s(x)$ and $t(x)$ when multiplied give sums of powers of u^k, the product is in T.

Let $z \in T$. Let $z = h(x)$ where $h(x)$ is a nonzero polynomial of degree less than n. Since $p(x)$ is irreducible, the greatest common divisor of $p(x)$ and $h(x)$ is 1. Then there are polynomials $r(x)$ and $s(x)$ such that $p(x)r(x) + h(x)s(x) = 1$. Let $x = u$. Then $1 = p(u)r(u) + h(u)s(u) = 0 + h(u)s(u)$ since $p(u) = 0$. Thus $s(u)$ is the inverse of $h(u)$. Hence T is a subfield of $F(u)$ and T contains u. But $F(u)$ is the smallest subfield containing u and F, so $T = F(u)$. Thus 1, $u, \ldots, u^{n-1}$ spans $F(u)$ and hence is a basis for $F(u)$ over F.

(4) From (3), the basis for $F(u)$ over F contains n elements and therefore $[F(u):F] = n$.

(5) Let $q(x) \in F[x]$. Suppose $q(u) = 0$ and $q(x)$ is not a multiple of $p(x)$. Since $p(x)$ is irreducible over F, the greatest common divisor of $p(x)$ and $q(x)$ is 1. Then there are polynomials $r(x)$, $s(x) \in F[x]$ such that $p(x)r(x) + q(x)s(x) = 1$. Let $x = u$. Then $1 = p(u)r(u) + q(u)s(u) = 0$ since $p(u) = 0$ and $q(u) = 0$. But this is a contradiction so $q(x)$ must be a multiple of $p(x)$.

Now suppose $q(x)$ is a multiple of $p(x)$. Then there is a nonzero polynomial $r(x) \in F[x]$ such that $q(x) = r(x)p(x)$. Let $x = u$. Then $q(u) = r(u)p(u) = 0$ since $p(u) =0$.

2.12 DEFINITION. Let K be an extension of a field F and u, $v \in K$. Let $F(u)$ and $F(v)$ be subfields of K. Then $F(u,v)$ denotes the intersection of all the subfields of K containing both $F(u)$ and $F(v)$.

2.13 THEOREM. Let K be an extension of a field F and u, $v \in K$. Then $F(u,v)$ is the smallest subfield of K containing both $F(u)$ and $F(v)$.

Proof: This result follows from 2.9.

2.14 REMARK. The subfield $F(u,v)$ may be considered in three ways:

(1) the smallest subfield containing F, u, and v

(2) the result of adjoining v to $F(u)$

(3) the result of adjoining u to $F(v)$.

2.15 DEFINITION. Let F be a field. If $p(x) \in F[x]$ can be factored into linear factors in a finite extension K of F but cannot be factored into linear factors in any proper subfield of K, then K is called a *splitting field* of $p(x)$, and it is said that $p(x)$ *splits* in K.

2.16 EXAMPLE. Find the splitting field of $p(x) = (x^2 + 5)(x^2 - 2)$ over $\mathcal{Q}$. Factor $p(x)$ into linear factors. Then

$$p(x) = (x - i\sqrt{5})(x + i\sqrt{5})(x - \sqrt{2})(x + \sqrt{2})$$

where $i = \sqrt{-1}$. Let $u = i\sqrt{5}$. Clearly $\mathcal{Q}(u)$ is the same field as $\mathcal{Q}(-u)$ since for any $\alpha \in \mathcal{Q}(-u)$, $\alpha = a + b(-u) = a - bu$ and $-b \in \mathcal{Q}$. Thus consider $\mathcal{Q}(u)$ as the splitting field of $x^2 + 5$. But $\mathcal{Q}(u)$ is not the splitting field of $x^2 - 2$. So adjoin $\sqrt{2}$ or $\sqrt{-2}$ to $\mathcal{Q}(u)$. Let $v = \sqrt{2}$. Then the splitting field of $p(x)$ is $\mathcal{Q}(uv) = \mathcal{Q}(u,v)$.

The two following theorems are stated here without proof and will be used later in the paper.

2.17 THEOREM. Let ϕ be an isomorphism of a field F onto a field F' with $\phi(c) = c'$ for all $c \in F$. Let $p(x) \in F[x]$ be irreducible and $p'(x)$ be the corresponding polynomial over F'. Let u, u' be roots of $p(x)$, $p'(x)$ respectively. Then there exists an isomorphism ϕ' from $F(u)$ onto $F'(u)$ such that $\phi'(u) = u'$ and $\phi'(c) = c'$ for all $c \in F$.

Proof: [5]

2.18 THEOREM. Let ϕ be an isomorphism of a field F onto a field F' with $\phi(c) = c'$ for all $c \in F$. Let $p(x) \in F[x]$ and $p'(x)$ be the corresponding polynomial over F'. Let K, K' be the splitting fields of $p(x)$, $p'(x)$ over F, F' respectively. Then there exists an isomorphism ϕ' of K onto K' such that $\phi'(c) = c'$ for all $c \in F$.

Proof: [5]

2.19 THEOREM. Let $p(x)$ be a polynomial over a field F and $p'(x) = 0$, where $p'(x)$ is the derivative of $p(x)$. Then $p(x) = a$ for some $a \in F$.

Proof: Suppose $p(x) \neq a$ for any $a \in F$. Then $p(x) = \sum_{i=0}^{n} \alpha_i x^i$ where $\alpha_i \in F$, $\alpha_n \neq 0$, and $n \geq 1$. Hence the derivative of $p(x)$ is $p'(x) = \sum_{i=1}^{n} i\alpha_i x^{i-1}$. But $n \neq 0$, $\alpha_n \neq 0$, and $x^{n-1} \neq 0$, so $p'(x) \neq 0$. This is a contradiction; hence $p(x) = a$ for some $a \in F$.

2.20 LEMMA. Let K be an extension of a field F. If $p(x)$, $q(x) \in F[x]$ have a nontrivial common factor in $K[x]$, then they have a nontrivial common factor in $F[x]$.

Proof: Let $p(x)$ and $q(x)$ have a nontrivial common factor in $K[x]$. Suppose they have no nontrivial common factor in $F[x]$. Then there exists $r(x)$, $s(x) \in F[x]$ such that $r(x)p(x) + s(x)q(x) = 1$. But $r(x)$, $s(x) \in F[x]$, so $p(x)$ and $q(x)$ must also be relatively prime in $K[x]$. Contradiction. Hence $p(x)$ and $q(x)$ have a nontrivial common factor in $F[x]$.

2.21 THEOREM. Let F be a field. A polynomial $p(x) \in F[x]$ has a multiple root if and only if $p(x)$ and $p'(x)$ have a nontrivial common factor.

Proof: Without loss of generality, assume the roots of $p(x)$ are in F, by 2.20. Let $p(x) \in F[x]$ be of degree $n > 0$ with multiple root u. Thus $p(x) = (x - u)^m q(x)$ where $q(x) \in F[x]$ and $m > 1$. Then

$$\begin{aligned} p'(x) &= m(x - u)^{m-1}q(x) + (x -u)^m q'(x) \\ &= (x - u)^{m-1}(mq(x) + (x - u)q'(x)). \end{aligned}$$

Clearly $x - u$ is a common factor of $p(x)$ and $p'(x)$.

For the converse, let $p(x)$ and $p'(x)$ have a common factor $x - u_k$. Suppose $p(x)$ has no multiple roots. Then there are n distinct roots u_i where $i = 1, . . . n$, of $p(x)$ and thus $p(x) = \prod_{i=1}^{n} (x - u_i)$. But $p'(x) = \sum_{j=1}^{n} (\prod_{\substack{i=1 \\ i \neq j}}^{n} (x - u_i))$. Since $x - u_k$ is a common factor, u_k is a root of $p(x)$ and $p'(x)$. Clearly $p(u_k) = 0$. But $p'(u_k) \neq 0$ since there is exactly one term in $p'(u_k)$ which is not equal to zero, namely $\prod_{\substack{i=1 \\ i \neq k}}^{n} (u_k - u_i) \neq 0$. This is a contradiction. Hence $p(x)$ must have a multiple root.

<u>2.22 THEOREM</u>. Let F be a field of characteristic zero. If $p(x)$ is irreducible over F, then $p(x)$ has no multiple roots.

<u>Proof</u>: Let $p(x)$ $F[x]$ be irreducible and suppose $p(x)$ has a multiple root u. Since $p(x)$ is irrdeucible, its only factors are 1 and $p(x)$. By 2.21, $p(x)$ and $p'(x)$ have a nontrivial common factor. Thus u is a root of $p(x)$ and $p'(x)$. By 2.11 (5), $p'(x)$ must be a multiple of $p(x)$. But then the degree of $p'(x)$ is greater than the degree of $p(x)$ or $p'(x) = 0$. Clearly $p'(x) = 0$ since by definition, the degree of $p'(x)$ is less than the degree of $p(x)$. Then $p(x)$ is a constant and has no roots. Thus $p(x)$ has no multiple roots.

2.23 DEFINITION. The extension K of a field F is called a simple extension of F if $K = F(u)$ for some $u \in K$.

2.24 THEOREM. Let F be a field of characteristic zero. If u_i for $i = 1, . . . n$ are algebraic over F, then there exists c in $F(u_1, . . . , u_n)$ such that $F(c) = F(u_1, . . . , u_n)$, that is, the extension is simple.

Proof: If $n = 1$, clearly $F(u_1) = F(u_1)$. Suppose $n = 2$. Let u, v be algebraic over F. Let $p(x)$ and $q(x)$ be the minimal irreducible polynomials over F of degree m and n satisfied by u, v respectively. Let K be the splitting field of both $p(x)$ and $q(x)$. Since $p(x)$ and $q(x)$ are irreducible and since F has characteristic zero, then neither $p(x)$ nor $q(x)$ has a multiple root by 2.22. Let the roots of $p(x)$ be $u = u_i$ for $i = 1, . . . , m$ and the roots of $q(x)$ be $v = v_j$ for $j = 1, . . . , n$. Suppose $j \neq 1$; then $v_j \neq v_1 - v$. Then there is exactly one solution λ_{ij} in K such that $u_i + \lambda_{ij}v_j = u_1 + \lambda_{ij}v_1 = u + \lambda_{ij}v$ for all $i = 1, . . . , m$. Solving this equation, $\lambda_{ij} = (u - u_i)/(v_j - v)$. But F is infinite, so there is a $\gamma \in F$ such that $\gamma \neq \lambda_{ij}$ for all $i = 1, . . . , m$ and $j \neq 1$. Then $u_i + v_j \neq u + v$. Let $c = u + v$. Clearly $c \in F(u,v)$, so $F(c) \subset F(u,v)$.

Now show that u, $v \in F(c)$. Since v is a root of $q(x)$ over F, it is a root of $q(x)$ over $F(c)$. Define a polynomial $h(x)$ by $h(x) = p(c - \gamma x)$. Let $x = v$. Then $h(v) = p(c - \gamma v) = p(u) = 0$. Thus v satisfies $h(x)$ over $F(c)$. Therefore, there is an extension field K of $F(c)$ which contains the common factor $x - v$ of $p(x)$

and $q(x)$. Suppose $v_j \neq v$ is another root of $q(x)$. Since $c \neq u_i + \gamma v_j$ for all $i = 1, \ldots, m$, $h(v_j) = p(c - \gamma v_j) \neq p(u_i) = 0$, and hence v_j is not a root of $h(x)$. Thus v is the only common root of $q(x)$ and $h(x)$, and $x - v$ is the only common factor since $q(x)$ has no multiple roots. Hence $x - v$ is the greatest common divisor of $q(x)$ and $h(x)$ over K. Then there is a nontrivial greatest common divisor of $q(x)$ and $h(x)$ over $K = F(c)$. But $x - v$ is the only nontrivial divisor of $x - v$, so $x - v$ is a polynomial $F(c)$. Thus $v \in F(c)$. Also $u \in F(c)$ since $u = c - \gamma v$, and $c, v, \gamma \in F(c)$. Then $F(u,v) \subset F(c)$, and hence $F(c) = F(u,v)$.

Now assume the theorem is true for $n = k$. Then if u_i for $i = 1, \ldots, k$ are algebraic over F, there is an element c in $F(u_1, \ldots, u_k)$ such that $F(c) = F(u_1, \ldots, u_k)$. Suppose that u_i for $i = 1, \ldots, u_{k+1})$ are algebraic over F. Then $F(u_1, \ldots, u_k, u_{k+1}) = F(c, u_{k+1})$. But by the case for $n = 2$, there exists an element $c' \in F$ such that $F(c') = F(c, u_{k+1})$. Thus by induction, the theorem is true for all n.

<u>2.25 DEFINITION</u>. Let F be a field. A polynomial $p(x) \in F[x]$ is called *separable* if it has no multiple roots.

<u>2.26 DEFINITION</u>. Let K be an extension of a field F. Then an element u in K is called *separable* over F if it is a root of a separable polynomial over F.

<u>2.27 DEFINITION</u>. Let K be an extension of a field F. Then K is called a *separable extension* of F if every element of K is separable over F.

2.28 DEFINITION. A field F is called perfect if every finite extension of F is a separable extension.

2.30 LEMMA. Let F be a field of characteristic zero. Then every irreducible polynomial $p(x)$ over F is separable.

Proof: Let $p(x) \in F[x]$ be irreducible. By 2.22 $p(x)$ has no multiple roots. Hence $p(x)$ is separable.

2.31 THEOREM. Every field F of characteristic zero is perfect.

Proof: Let F be a field of characteristic zero and let K be a finite extension of F. Let $u \in K$. Let $p(x) \in F[x]$ be a polynomial of minimal degree with root u. By 2.11, $p(x)$ is irreducible. Then u is separable over F, and K is separable. Thus F is a perfect field.

2.32 THEOREM. Let F be a field of characteristic zero and K be a finite extension of F. Then $u \in K$ is algebraic over F if and only if u is separable over F.

Proof: Let $u \in K$ be algebraic over F. Since F is of characteristic zero, F is perfect and hence K is a separable extension of F. But then every element of K is separable over F, so u is separable over F.

Now assume $u \in K$ is separable over F. Let $p(x) \in F[x]$ be a polynomial of minimal degree such that u is a root of $p(x)$. Then $p(u) = o$ and hence u is algebraic over F.

2.33 THEOREM. Let F be a field of characteristic zero, and let K be an extension of F. Then $u \in K$ is algebraic over F if and only if $F(u)$ is a finite extension of F.

Proof: Let $u \in K$ and assume $F(u)$ is a finite extension of F. Since F is perfect, $F(u)$ is a separable extension of F. Hence u is separable over F. Then by 2.32, u is algebraic over F.

For the converse, assume $u \in K$ is algebraic over F. Then u satisfies some polynomial over F. Let $p(x) \in F[x]$ be a monic polynomial of minimal degree n such that $p(u) = 0$. Then by 2.11 (4), $[F(u):F] = n$. Hence by definition of $F(u)$ is a finite extension of F.

2.34 THEOREM. Let F be a field of characteristic zero. If K is a finite, separable extension of F, then K is a simple extension.

Proof: Let K be a finite, separable extension of F. Then $K = F(u_1, \ldots, u_n)$ where $u_i \in K$ for $i = 1, \ldots, n$. But the u_i are separable over F, and hence by 2.32, are algebraic over F. Since F is of characteristic zero, it follows from 2.24 that there is a $c \in F(u_1, \ldots, u_n) = K$ such that $F(c) = K$. Thus K is a simple extension of F.

2.35 EXAMPLE. Find $c \in \mathcal{Q}(\sqrt{2}, \sqrt{3})$ such that $\mathcal{Q}(c) = \mathcal{Q}(\sqrt{2}, \sqrt{3})$. Let $u = \sqrt{2}$ and $v = \sqrt{3}$. Since $\mathcal{Q}$ is of characteristic zero and $\mathcal{Q}(u,v)$ is a finite extension of $\mathcal{Q}$, $\mathcal{Q}(u,v)$ is a separable extension of $\mathcal{Q}$. Thus u and v are separable over $\mathcal{Q}$ and hence algebraic over $\mathcal{Q}$. Then $p(x) = x^2 - 2$ and $q(x) = x^2 - 3$ are polynomials of minimal degree over $\mathcal{Q}$ such that and u and v are roots of $p(x)$ and $q(x)$ respectively. Let the roots of $p(x)$ be denoted by $u_1 = u$, $u_2 = -u$. Let the roots of $q(x)$ be denoted by $v_1 = v$, $v_2 = -v$. Clearly $p(x)$ and $q(x)$ are separable polynomials. For $j \neq 1$, the only $v_j = v_2$. Then for each i, there is exactly one solution λ_{ij} in $\mathcal{Q}(u,v)$ such that $u_i + \lambda_{ij}v_j = u_i + \lambda_{ij}v_2 = u_1 + \lambda_{ij}v_1$. Thus, solving the equation, $\lambda_{ij} = (u_1 - u_i)/(v_2 - v_1)$. Then for $i = 1$, $\lambda_{ij} = \lambda_{12} = 0$ and for $i = 2$, $\lambda_{ij} = \lambda_{22} = -u/u$. Since $\mathcal{Q}$ is of characteristic zero, there is $\gamma \in \mathcal{Q}$ such that $\gamma \neq \lambda_{ij}$ and $u_i + \gamma v_2 \neq u_1 + \gamma v_1$. Let $c = u_1 + \gamma v_1$, and let $\gamma = -1$. Hence $c = u_1 - v_1 = u - v$. Then $\mathcal{Q}(u - v) \subset \mathcal{Q}(u,v)$. Define $h(x) = p(c - x) = p(u - v + x) = x^2 - 2xv + 2xu - 2uv + 3$. So $h(x)$ is a polynomial over $\mathcal{Q}(u - v)$. Let $x = v$. Then $h(v) = 0$, and v is a root of $h(x)$. Thus $x - v$ is a common divisor of $h(x)$ and $q(x)$ in an extension K of $\mathcal{Q}(u - v)$. But $-v$ is not a root of $h(x)$, so $x + v$ is not a common divisor of $h(x)$ and $q(x)$. Thus $x - v$ is the greatest common divisor of $h(x)$ and $q(x)$ over K, and hence over $\mathcal{Q}(u - v)$ since $x - v$ is the only nontrivial divisor of itself. Then $x - v$ is a polynomial over $\mathcal{Q}(u - v)$, which implies u is in $\mathcal{Q}(u - v)$. Clearly $u \in \mathcal{Q}(u - v)$ since $u = c + v$ and v, c are in $\mathcal{Q}(u - v)$. Then $\mathcal{Q}(u,v) \subset \mathcal{Q}(u - v)$, and $c = u - v$ satisfies the conditions.

CHAPTER III

AUTOMORPHISMS AND FIXED FIELDS

3.1 DEFINITION. The group of all automorphisms for a field F is called the automorphism group of F.

3.2 EXAMPLE. Find the automorphism group of $\mathcal{Q}$. Let ϕ be an automorphism of $\mathcal{Q}$. By the properties of isomorphisms, $\phi(0) = 0$ and $\phi(1) = 1$. Assume $\phi(k) = k$ for the positive integer k. Then by induction, $\phi(k + 1) = \phi(k) + \phi(1) = k + 1$. Hence ϕ maps every positive integer into itself. Again by the properties of isomorphisms, $\phi(-k) = -k$ and $\phi(k^{-1}) = k^{-1}$ for all positive integers k. Thus ϕ maps every integer into itself. Let m and $n \neq 0$ be integers. Then $m/n \in \mathcal{Q}$ and $\phi(m/n) = \phi(mn^{-1}) = \phi(m)\phi(n^{-1}) = mn^{-1} = m/n$. Hence ϕ maps every rational into itself and is the identity map I. Clearly this is the only automorphism of $\mathcal{Q}$, so the automorphism group is $\{I\}$.

3.3 EXAMPLE. Find the automorphism group of $\mathcal{Q}(\sqrt{5})$. Let $u = \sqrt{5}$. Let I be the identity map. Define a map α by $\alpha(a + bu) = a - bu$ where $a, b \in \mathcal{Q}$. Clearly α is one-to-one and onto. Let $(a + bu)$, $(c + du) \in \mathcal{Q}(u)$. Then

$$\begin{aligned} \alpha((a + bu) + (c + du)) &= \alpha((a +c) + (b + d)u) \\ &= (a + c) - (b + d)u \\ &= (a - bu) + (c - du) \\ &= \alpha(a + bu) + \alpha(c + du) \end{aligned}$$

and

$$\begin{aligned}\alpha((a + bu)(c + du)) &= \alpha(ac + bcu + adu + 5bd)\\ &= (ac + 5bd) - (bc + ad)u\\ &= c(a - bu) - d(a - bu)u\\ &= (a - bu)(c - du)\\ &= \alpha(a + bu)\alpha(c + du).\end{aligned}$$

Hence α is an automorphism. Assume there is another automorphism τ. Then $\tau(u^2) = \tau(5) = 5$ and $\tau(u^2) = \tau(uu) = \tau(u)\tau(u)$. Thus $\tau(u)\tau(u) = 5$. Now $\tau(a + bu) = \tau(a) + \tau(bu) = a + b\tau(u)$, since I is the only automorphism of $\mathcal{Q}$, and $\tau(u) = u$ or $\tau(u) = -u$. But then either $\tau(a + bu) = a + bu$, which is just I, or $\tau(a + bu) = a - bu$, which is α. Hence the automorphism group of $\mathcal{Q}(u)$ is $\{I,\alpha\}$.

3.4 DEFINITION. Let K be a field and G be the automorphism group of K. If H is a subgroup of G, the set H' of elements of K whose elements remain fixed under the automorphisms of H is called the _fixed_ _field_ of H, that is, $H' = \{a \in K \mid \phi(a) = a \text{ for all } \phi \in H\}$.

3.5 THEOREM. The fixed field H' of H is a subfield of K.

Proof: Let H' be the fixed field of H. Let a, $b \in H'$. Then $a + (-b) = \phi(a) + \phi(-b) = \phi(a - b)$ for all $\phi \in H$. Hence $a - b \in H'$. Now suppose $b \neq 0$. Then $ab^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$ for all $\phi \in H$. Thus $ab^{-1} \in H'$, and hence H is a subfield of K.

3.6 DEFINITION. Let K be a field and G be a group of automorphisms of K. If F is a subfield of K, the set F' of all automorphisms of K which leave every element in F fixed is called the group of automorphisms of K relative to F, that is, $F' = \{\phi \in G \mid \phi(a) = a$ for all $a \in F\}$.

3.7 THEOREM. The group of automorphisms F' of K relative to a subfield F is a subgroup of G, the automorphism group of K, under composition of mappings.

Proof: Let F' be the group of automorphisms of K relative to F. Let $\phi, \tau \in F'$ and $a \in F$. Since $I(a) = a$, $I \in F'$. Now $\phi\tau^{-1}(a) = \phi(\tau^{-1}(a)) = \phi(\tau^{-1}(\tau(a))) = \phi(a) = a$. Thus $\phi\tau^{-1} \in F'$, and F' is a subgroup of G.

3.8 EXAMPLE. Consider the field $\mathcal{Q}(u,v)$ where $u = \sqrt{5}$ and $v = \sqrt{2}$. Then any element in the field is of the form $a + bu + cv + duv$ where $a, b, c, d \in \mathcal{Q}$. Let I be the identity automorphism. Consider the field as $(\mathcal{Q}(v))(u)$. Then σ_1: $a + bu \to a - bu$ is an automorphism of $\mathcal{Q}(u,v)$ where $a, b \in \mathcal{Q}(v)$. Also, $\mathcal{Q}(v)$ is the fixed field of σ_1. Now consider $\mathcal{Q}(u,v)$ as $(\mathcal{Q}(u))(v)$. Similarly, there is an automorphism σ_2: $a + bv \to a - bv$ where $a, b \in \mathcal{Q}(u)$, with fixed field $\mathcal{Q}(u)$. By 1.4, the composition of automorphisms is an automorphism. Define σ_3 by $\sigma_3 = \sigma_1\sigma_2 = \sigma_2\sigma_1$. Then

σ_3: $a + bu + cv + duv \to a - bu - cv + duv$. The fixed field of σ_3 is $\mathcal{Q}$.

Let $G = \{I, \sigma_1, \sigma_2, \sigma_3\}$. Clearly G is a group under composition of mappings. As in 3.3, there are no other automorphisms of $\mathcal{Q}(u,v)$, so G is the group of all automorphisms and $\mathcal{Q}$ is its fixed field. Now to illustrate 2.5, compute $[\mathcal{Q}(u,v):\mathcal{Q}]$. Since $\mathcal{Q} \subset \mathcal{Q}(u) \subset \mathcal{Q}(u,v)$,

$[\mathcal{Q}(u,v):\mathcal{Q}] = [\mathcal{Q}(u,v):\mathcal{Q}(u)][\mathcal{Q}(u):\mathcal{Q}]$. Any element in $\mathcal{Q}(u,v)$ over $\mathcal{Q}(u)$ is of the form $a + bv$ where a, $b \in \mathcal{Q}(u)$. So $\{1,v\}$ is a basis and $[\mathcal{Q}(u,v):\mathcal{Q}(u)] = 2$. Since any element of $\mathcal{Q}(u)$ over $\mathcal{Q}$ is of the form $a + bu$, where a, $b \in \mathcal{Q}$, a basis is $\{1,u\}$. Hence $[\mathcal{Q}(u):\mathcal{Q}] = 2$. So $[\mathcal{Q}(u,v):\mathcal{Q}] = (2)(2) = 4$.

<u>3.9 THEOREM</u>. Let N be a field with subfields K, L, M such that $K \subset L \subset M \subset N$. Let G be the group of automorphisms of K with subgroups J and H such that $J \subset H \subset G$. Then

(1) $L \subset M$ implies $L' \supset M'$

(2) $J \subset H$ implies $J' \supset H'$.

<u>Proof</u>: (1) Let L', M' be the automorphism groups of N relative to L and M, respectively. Let $\phi \in M'$. Then $\phi(a) = a$ for all $a \in M$. Since $L \subset M$, ϕ must also leave every element of L fixed. Then $\phi \in L'$. Hence $M' \subset L'$.

(2) Let J', M' be the fixed fields of J and H respectively. Let $a \in H'$. Then $\phi(a) = a$ for all $\phi \in H$. Since $J \subset H$, every element in J also leaves a fixed. Then $a \in J'$ and $H' \subset J'$.

<u>3.10 DEFINITION</u>. Let H be a subgroup of the group of automorphisms of a field K and let H' be the fixed field of H. Then the <u>closure</u> of H, denoted H'', is the group of automorphisms of K relative to H'.

<u>3.11 DEFINITION</u>. Let F be a subfield of a field K and let F' be the group of automorphisms of K relative to F. Then the <u>closure</u> of F, denoted F'', is the fixed field of F'.

3.12 DEFINITION. A subfield F of a field K or a subgroup H of the group of automorphisms of K is called closed if and only if $F = F''$ or $H = H''$ respectively.

3.13 THEOREM. Let F be a subfield of a field K and let F' be the group of automorphisms of K relative to F. Then

(1) $F \subset F''$

(2) $F' \subset F'''$.

Proof: (1) Let $a \in F$ and let F'' be the fixed field of F'. Then $\phi(a) = a$ for all $\phi \in F'$. Then clearly $a \in F''$. Hence $F \subset F''$.

(2) Let F''' be the group of automorphisms of K relative to F'' and let $\phi \in F'$. Then $\phi(a) = a$ for all $a \in F$. But then $a \in F''$, and hence $\phi \in F'''$. Thus $F' \subset F'''$.

3.14 THEOREM. Let K be a field and let G be the group of automorphisms of K. Let F be a closed subfield of K with F' the group of automorphisms of K relative to F. Then the fixed field of F' is F.

Proof: Let $a \in F$. Let L denote the fixed field of F'. Then $\phi(a) = a$ for all $\phi \in F'$. Hence $a \in L$, and $F \subset L$. Let L' be the group of automorphisms of K relative to L. Let $a \in L$. Then since L is the fixed field of F', $\phi(a) = a$ for all $\phi \in F'$. But $\phi \in L'$, so $F' \subset L'$. By part (2) of 3.13, $L'' \subset F''$. Since F is closed, $F = F''$. Hence $L \subset L'' \subset F'' = F$. Thus $L = F$.

<u>3.15 THEOREM</u>. Let K be a field and G be the group of automorphisms of K. Let H be a closed subgroup of G with fixed field H'. Then the group of automorphisms of K relative to H' is H.

<u>Proof</u>: Let $\phi \in H$. Let J denote the group of automorphisms of K relative to H'. Then $\phi(a) = a$ for all $a \in H'$. Hence $\phi \in J$, and $H \subset J$. Now let $\phi \in J$. Let J' be the fixed field of J. Clearly if $a \in H'$, then $a \in J'$. Hence $H' \subset J'$. Then by part (2) of 3.13, $J'' \subset H''$. But $H = H''$ since H is closed. Thus $J \subset J'' \subset H'' = H$. Then $J = H$.

<u>3.16 THEOREM</u>. Let K be a field. Let $F \rightarrow F'$ be a mapping from the ordered structure $(\mathcal{F},\subset)$ of all closed subfields of K onto the ordered structure $(\mathcal{H},\supset)$ of all closed subgroups of the group of automorphisms of K. Then the mapping is a one-to-one correspondence, and its inverse is $H \rightarrow H'$.

<u>Proof</u>: Let ϕ be a mapping of $(\mathcal{F},\subset)$ into $(\mathcal{H},\supset)$, defined by $\phi(F) = F'$, where $F \in (\mathcal{F},\subset)$. Let F_1 and F_2 be closed subfields of K. Assume $\phi(F_1) = \phi(F_2)$. Then $F_1' = F_2'$. Hence the fixed field of F_1' must be the fixed field of F_2', that is, $F_1'' = F_2''$. But since F_1 and F_2 are closed, $F_1 = F_1'' = F_2'' = F_2$. Thus ϕ is one-to-one.

Now let H be a closed subgroup in $(\mathcal{H},\supset)$. Then ϕ is onto if there exists a subfield E of K such that $\phi(E) = H$. Let $E = H'$, the fixed field of H. Then $\phi(E) = \phi(H') = H'' = H$ since H is closed. Thus ϕ is a one-to-one correspondence.

Let τ be a mapping from $(\mathcal{H},\supset)$ into $(\mathcal{F},\subset)$, defined by $\tau(H) = H^{'}$. Then $\phi(\tau(H)) = \phi(H^{'}) = H^{''} = H$ since H is closed. Thus $\tau = \phi^{-1}$; so the inverse of ϕ maps $H \to H^{'}$.

CHAPTER IV

NORMAL EXTENSIONS

Let the field F be of characteristic zero throughout this chapter.

4.1 THEOREM. Let F be a field and $F(x_1, \ldots, x_n)$ be the field of rational functions in $x_1, \ldots, x_n$ over F. Let $\sigma \in S_n$, the symmetric group of degree n, and $r(x_1, \ldots, x_n)$ be in $F(x_1, \ldots, x_n)$. Define a mapping $\bar{\sigma}$ of $F(x_1, \ldots, x_n)$ onto itself by $\bar{\sigma}: r(x_1, \ldots, x_n) \to r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Then $\bar{\sigma}$ is an automorphism.

Proof: By definition, $\bar{\sigma}$ is one-to-one and onto. Let $r(x_1, \ldots, x_n)$ and $s(x_1, \ldots, x_n)$ be in $F(x_1, \ldots, x_n)$ and $\sigma \in S_n$. Since $F(x_1, \ldots, x_n)$ is a field, the sum and product of rational functions in $x_1, \ldots, x_n$ are also rational functions in $x_1, \ldots, x_n$. Then

$$\begin{aligned} &\bar{\sigma}(r(x_1, \ldots, x_n) + s(x_1, \ldots, x_n)) \\ &= r + s(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \\ &= r(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) + s(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \\ &= \bar{\sigma}(r(x_1, \ldots, x_n)) + \bar{\sigma}(s(x_1, \ldots, x_n)) \end{aligned}$$

and

$$\begin{aligned} &\bar{\sigma}(r(x_1, \ldots, x_n)s(x_1, \ldots, x_n)) \\ &= rs(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \end{aligned}$$

$$= r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})s(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$
$$= \bar{\sigma}(r(x_1, \ldots, x_n))\bar{\sigma}(s(x_1, \ldots, x_n)).$$

Hence $\bar{\sigma}$ is an automorphism.

4.2 COROLLARY. The set of all automorphisms of $F(x_1, \ldots, x_n)$ relative to F is a group.

Proof: The result follows immediately from 3.7.

4.3 DEFINITION. An element of $F(x_1, \ldots, x_n)$ left fixed by all $\bar{\sigma}$ defined by $\sigma \in S_n$ is called a symmetric rational function in $x_1, \ldots, x_n$ over F.

4.4 THEOREM. Let F be a field and $F(x_1, \ldots, x_n)$ be the field of rational functions in $x_1, \ldots, x_n$ over F. Then the fixed field of $F(x_1, \ldots, x_n)$ with respect to S_n is the set of all symmetric rational functions in $x_1, \ldots, x_n$ over F.

Proof: By definition, the set of elements left fixed by all elements in S_n is precisely the set of symmetric rational functions.

4.5 COROLARY. The set of symmetric rational functions is a subfield of $F(x_1, \ldots, x_n)$.

Proof: This follows from 3.5.

4.6 DEFINITION. The elementary symmetric functions in $x_1, \ldots, x_n$ are defined to be

$$a_1 = \sum_{i=1}^{n} x_i$$

$$a_2 = \sum_{i_1<i_2} x_{i_1}x_{i_2}$$

$$\begin{matrix} . & . & . \\ . & . & . \\ . & . & . \end{matrix}$$

$$a_n = x_1 \cdot \cdot \cdot \cdot x_n$$

$$a_r = 0 \quad \text{for all} \quad r > n.$$

4.7 THEOREM. Let F be a field and $F(x_1, \ldots, x_n)$ be the field of rational functions in $x_1, \ldots, x_n$ over F. Then the elementary symmetric functions in $x_1, \ldots, x_n$ over F are symmetric rational functions.

Proof: Let $\sigma \in S_n$ and $\bar{\sigma}$ be an automorphism of $F(x_1, \ldots, x_n)$. Assume the x_i are all distinct and let $p(x)$ in $F[x]$ be defined by

$$p(x) = \prod_{i=1}^{n} (x - x_i) = x^n - (\sum_{i=1}^{n} x_i)x^{n-1} + \ldots + (-1)^n x_1 \ldots x_n.$$

Then $\bar{\sigma}(p(x)) = \prod_{i=1}^{n} (x - x_{\sigma(i)}) = p(x)$ since $\sigma(i)$ is just a permutation of $1, \ldots, n$ and the factors of $p(x)$ are commutative. Hence the coefficients of $p(x)$ remain fixed. But the coefficients are precisely 1 and the elementary symmetric functions. Thus the elementary symmetric functions are symmetric.

4.8 DEFINITION. Let F be a field. If K is a finite extension of F such that F is the fixed field of the group of automorphisms of K relative to F, then K is called a normal extension.

4.9 THEOREM. Let F be a field and K be a finite extension of F. Then K is a normal extension of F if and only if F is a closed subfield of K.

Proof: Let F' be the group of automorphisms of K relative to F and F'' be the fixed field of F'. Suppose that K is a normal extension of F. Then F is the fixed field of F'. But the fixed field of F' is F'', so $F = F''$. Hence F is closed.

Now suppose F is closed. Then F is the fixed field of F'. Since K is a finite extension of F, by definition, K is a normal extension of F.

4.10 THEOREM. Let K be a finite extension of a field F. Then the group of automorphisms F' of K relative to F is finite, and its order $o(F')$ satisfies $o(F') \leq [K:F]$.

Proof: Let $[K:F] = n$ and let u_i for $i = 1, . . n$ be a basis for K over F. Suppose the order of F' is $n + 1$. Then there are $n + 1$ automorphisms ϕ_j in F', where $j = 1, . . n + 1$. Consider the system of n homogeneous equations in $n + 1$ unknowns

$$\phi_1(u_i)x_1 + . . . + \phi_{n+1}(u_i)x_{n+1} = 0,$$

where $i = 1, . . . , n$. From 1.6, this system has a nontrivial solution $x_j = a_j$ in K, $j = 1, . . . , n + 1$, that is, not all $x_j = 0$. Then $\phi_i(u_i)a_1 + . . . + \phi_{n+1}(u_i)a_{n+1} = 0$ for all $i = 1, . . n$.

Let $t \in K$. Since u_i, $i = 1, . . . , n$, is a basis for K over F, $t = c_1u_1 + . . . + c_nu_n$ where $c_i \in F$ Then, since ϕ_i leaves c_i fixed,

$$\begin{aligned}\sum_{j=1}^{n+1} \phi_j(t)a_j &= \sum_{j=1}^{n+1} a_j\ \phi_j(\ \sum_{i=1}^{n} c_iu_i) \\ &= \sum_{j=1}^{n+1}\ \sum_{i=1}^{n} a_jc_i\phi_j(u_i) \\ &= \sum_{i=1}^{n} c_i(\ \sum_{j=1}^{n+1} a_j\phi_j(u_i) \\ &= \sum_{i=1}^{n} c_i0 \\ &= 0\end{aligned}$$

for all $t \in K$. But this contradicts 1.7. Then $o(F') \neq n + 1$. Thus $o(F') \leq n = [K:F]$.

4.11 THEOREM. Let K be a normal (finite) extension of a field F and let H be a subgroup of F', the group of automorphisms of K relative to F. Let H' be the fixed field of H. Then

(1) $[K:H'] = o(H)$

(2) H is closed.

Proof: (1) Let H'' be the group of automorphisms of K relative to H'. By 3.13, $H \subset H''$, so $o(H) \leq o(H'')$. Then by 4.10, $o(H'') \leq [K:H']$. Thus $o(H) \leq [K:H']$.

By 2.24, there is $u \in K$ such that $K = H'(u)$. Let $[K:H'] = n$. Then u satisfies an irreducible polynomial over H' of minimal degree n. Let $o(H) = h$. Then there are h distinct automorphisms of K relative to F in H. Denote these by ϕ_i, where $i = 1, . . . , h$ and ϕ_1 is the identity automorphism of F'. Thus $\phi_1(c) = c$ for all $c \in F$. Now consider the elementary symmetric functions in $\phi_i(c)$

defined by

$$a_1 = \sum_{i=1}^{h} \phi_i(c)$$

$$a_2 = \sum_{i_1<i_2} \phi_{i_1}(c)\phi_{i_2}(c)$$

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{matrix}$$

$$a_h = \phi_1(c) \; . \; . \; . \; \phi_h(c).$$

Let ϕ H. By 4.7, each a_i is a symmetric rational function. Hence $\phi(a_i) = a_i$ for all $\phi \in H$ and $i = 1, . . h$. Thus $a_i \in H'$ for all $i = 1, . . . , h$. Let $p(x)$ be a polynomial over H' defined by $p(x) = \prod_{i=1}^{h} (x - \phi_i(c)) = x^h - a_1x^{h-1} + . . . + (-1)a_h$ as in 4.7. Then for $x = c$, $x - \phi_1(c) = c - c = 0$. Thus $p(c) = 0$, and c is a root of $p(x)$. Since n is the minimal degree of an irreducible polynomial for which c is a root, $h \geq n$. Then $o(H) = h \geq n = [K:H']$, and hence $o(H) \geq [K:H']$. Thus $o(H) = [K:H']$.

(2) By 3.13, $o(H) \leq o(H'')$. From part (1), $o(H'') \leq [K:H'] = o(H)$. Hence $o(H'') \leq o(H)$. so $o(H'') = o(H)$. Since H is a subgroup of H'' with the same order of H'', $H = H''$. Then H is closed.

4.12 COROLLARY. If $H = F'$, then $[K:F] = o(F')$.

Proof: Let $H = F'$. Then $H' = F''$. But K is a normal extension of F, so by 4.9, $F = F''$. Hence $H' = F$. Then $[K:F] = [K:H'] = o(H)$.

4.13 LEMMA. Let F be a field, $f(x) \in F[x]$, and K be the splitting field of $f(x)$ over F. Let $p(x)$ be an irreducible factor of $f(x)$. If the roots of $p(x)$ are u_i, where $i = 1, \ldots, n$, then for each i, there exists an automorphism ϕ_i of K relative to F such that $\phi_i(u_1) = u_i$.

Proof: Let u_i, where $i = 1, \ldots, n$, be the roots of $p(x)$. Then each $u_i \in K$ and are roots of $f(x)$. Let u_1 and u_i be two roots of $p(x)$. Then there is an isomorphism τ of $F(u_1)$ onto $F'(u_1) = F(u_i)$ such that $\tau(u_1) = u_i$ and $\tau(c) = c$ for all $c \in F$ by 2.17. Now K is the splitting field of $f(x)$ over $F(u_1)$ and over $F(u_i)$. Then by 2.18, there is an isomorphism ϕ_i of K onto K, hence an automorphism, which coincides with τ on $F(u_1)$. In particular $\phi_i(u_1) = \tau(u_1) = u_i$ and $\phi(c) = \tau(c) = c$ for all $c \in F$.

4.14 THEOREM. K is a normal extension of a field F if and only if K is the splitting field of some polynomial over F.

Proof: Let F be a field. Assume K is a normal extension of F. Let F' be the group of automorphisms of K relative to F. Since K is a normal (finite) extension and F is of characteristic zero, by 2.24, there exists an element $c \in K$ such that $K = F(c)$. Let ϕ_i for $i = 1, \ldots, n$ be the elements in F', where ϕ_1 is the identity. Let a_i be the elementary symmetric functions in $\phi_i(c)$, $i = 1, \ldots, n$. Let $p(x) = \prod_{i=1}^{n} (x - \phi_i(c)) = x^n - a_1x^{n-1} + \ldots + (-1)a_n$ over K. Thus $p(x)$ factors into distinct linear factors over K. By 4.7, each a_i remains fixed under every $\phi \in F'$. Hence a_i form the fixed field of F'. But the fixed field of F' is F since K is a normal extension of F, so $a_i \in F$ for $i = 1, . . . n$. Then the coefficients of $p(x)$ are in F. Thus $p(x)$ is in $F[x]$. Clearly, c is a root of $p(x)$ since for $x = c$, $x - \phi_1(c) = c - c = 0$. Hence $p(c) = 0$. By 2.9, $F(c)$ is the smallest subfield containing both F and c. Since $K = F(c)$, K is the smallest subfield containing F and c. Thus c is in no proper subfield of K, and $p(x)$ cannot be factored into linear factors in any proper subfield of K. Hence K is the splitting field of $p(x)$ over F.

For the converse, let K be the splitting field of some polynomial $f(x)$ over F and proceed by induction on $[K:F]$. Let $[K:F] = n$. Assume that for any pair of fields K' and F', where $[K':F'] < n$, if K' is the splitting field of a polynomial over F', then K' is a normal extension of F'. Let $p(x) \in F[x]$ of degree $r > 1$ be an irreducible factor of $f(x)$. Since F is of characteristic zero, $p(x)$ is separable by 2.30. Hence the roots of $p(x)$ are all distinct. Let u_i, where $i = 1, . . . , n$, be the roots of $p(x)$. Consider u_1. Then K is the splitting field of $p(x)$ over $F(u_1)$. By 2.5,

$$[K:F(u_1)][F(u_i):F] = [K:F] = n.$$

But $[F(u_1):F] = r$; hence $[K:F(u_1)] = n/r < n$. By the induction hypothesis, K is a normal extension of $F(u_1)$.

Let x be any element in K which remains fixed under every in F'. At least one such x exists since 0 and 1 in F remain fixed. Any automorphism of K relative to $F(u_1)$ leaves F fixed since $F \subset F(u_1)$, and hence leaves x fixed. Then x is in the fixed field of K relative to $F(u_1)$. But K is a normal extension of $F(u_1)$ and so $x \in F(u_1)$. Thus $x = \sum_{j=0}^{r-1} c_j u_1^j$ where $c_j \in F$, by 2.11, (3).

By 4.13, for each i, there is a $\phi_i \in F'$ such that $\phi_i(u_1) = u_i$ and $\phi_i(c_j) = c_j$ for all $c_j \in F$. Then $x = \phi_i(x) = \sum_{j=0}^{r-1} c_j u_i^j$. Let $q(x) = (c_0 - x) + c_1 x + \ . \ . \ . + c_{r-1} x^{r-1}$. Then u_i for $i = 1, \ . \ . \ . \ ,$ n, are all distinct roots of $q(x)$. But then the number of roots is greater than the degree of $q(x)$. Hence the coefficients of $q(x)$ must be zeros. Then $c_0 - x = 0$ and $c_0 = x$. But $c_0 \in F$, so $x \in F$. This means F must be the fixed field of F'; hence K is a normal extension of F.

CHAPTER V

FUNDAMENTAL THEOREM OF GALOIS THEORY

Let the field F be of characteristic zero throughout this chapter.

5.1 DEFINITION. Let F be a field and $p(x) \in F[x]$. Let K be the splitting field of $p(x)$ over F. Then the group of automorphisms of K relative to F which leave every element of F fixed is called the Galois group of $p(x)$, and is denoted by $G(K,F)$.

5.2 THEOREM. Let F be a field, $p(x) \in F[x]$ be separable, and K be the splitting field of $p(x)$ over F. Then the Galois group of $p(x)$ is the group of permutations of the roots of $p(x)$.

Proof: Let $G(K.F)$ be the Galois group of $p(x)$. Let the roots of $p(x)$ be u_i, where $i = 1, \ldots, n$. Then by 4.13, for each i, there exists $\sigma_i \in G(K,F)$ leaving elements of F fixed such that $\sigma_i(u) = u_i$, $u = u_i$ for $i = 1, \ldots, n$.

Conversely, consider a root u of $p(x)$, where $p(x) = \sum_{i=0}^{n} c_i x^i$, for $c_i \in F$. Then for any $\sigma \in G(K,F)$,

$$p(\sigma(u)) = \sum_{i=0}^{n} c_i \sigma(u)^i$$

$$= \sum_{i=0}^{n} \sigma(c_i)\sigma(u)^i$$

$$= \sigma\left(\sum_{i=0}^{n} c_i u^i\right)$$

$$= \sigma(0)$$

$$= 0.$$

Hence each $\sigma \in G(K,F)$ is just the permutation of the roots.

5.3 FUNDAMENTAL THEOREM. Let F be a field and $p(x) \in F[x]$. Let K be the splitting field of $p(x)$ over F, and $G(K,F)$ be the Galois group of $p(x)$. Let T be a subfield of K containing F, and H be a subgroup of $G(K,F)$. Let $G(K,T) = \{\sigma \in G(K,F) \mid \sigma(t) = t$ for all $t \in T\}$ and $H' = \{x \in K \mid \sigma(x) = x$ for all $\sigma \in H\}$. Then the association of T with $G(K,T)$ sets up a one-to-one correspondence of the subfields of K which contain F onto the subgroups of $G(K,F)$ such that

(1) T is the fixed field of $G(K,T)$

(2) $H = G(K,H')$

(3) $[K:T] = o(G(K,T))$ and $[T:F]$ = index of $G(K,T)$ in $G(K,F)$

(4) T is a normal extension of F if and only if $G(K,T)$ is a normal subgroup of $G(K,F)$

(5) If T is a normal extension of F, then $G(T,F)$ is isomorphic to $G(K,F)/G(K,T)$.

Proof: Since K is the splitting field of $p(x)$ over F, it is the splitting field of $p(x)$ over any subfield which contains F. Hence K is the splitting field of $p(x)$ over T. Then by 4.14, is a normal extension of T. But then T is closed by 4.9, and by 4.11, $G(K.T)$ is closed. From 3.16, there exists a one-to-one correspondence of the closed subfields of K onto the closed subgroups of G(K,F). Hence there is a one-to-one correspondence of the subfields of K which contain F onto the subgroups of G(K,F).

(1) Since K is a normal extension of T, by definition, T is the fixed field of G(K,T).

(2) By 4.11, H is closed. Hence H is the group of automorphisms of K relative to H'. But this is precisely $G(K,H')$.

(3) Since K is a normal extension of both T and F, then $[K:T] = o(G(K,T))$ and $[K:F] = o(G(K,F))$ respectively by part (2) and 4.12. Now $[K:F] = [K:F][T:F]$ by 2.5. Hence

$o(G(K,F)) = o(G(K,T))[T:F]$.

Then $[T:F] = o(G(K,F))/o(G(K,T))$. Since K is the splitting field of p(x) over F, K is a finite extension of F. Then $[K:F] = o(G(K,F))$ is finite, and thus G(K,F) is finite. Then $o(G(K,F))/o(G(K,T))$ is the index of G(K,T) in G(K,F).

(4) First show T is a normal extension of F if and only if for all $\sigma \in G(K,F)$, $\sigma(T) \subset T$. Assume $\sigma(T) \subset T$. Since T is the splitting field of some polynomial over F, T is a finite extension of F. Hence by 2.24, there exists $u \in T$ such that $T = F(u)$. Then $\sigma(u) \in T$. Let σ_i for $i = 1, \ldots, n$ be the elements of G(K,F). Then, as in the preceding theorems, T is the splitting field of $p(x) = \prod_{i=1}^{n} (x - \sigma_i(u))$ which is in F[x]. Hence T is a normal extension of F.

Conversely, suppose T is a normal extension of F. Since T is a finite extension of F, there is an $u \in T$ such that $T = F(u)$ by

4.14, there is a minimal polynomial $p(x) \in F[x]$ of u with all its roots in T. But for all $\sigma \in G(K,F)$, $\sigma(u)$ is also a root of $p(x)$ by 4.13, and so $\sigma(u) \in T$. Since $T = F(u)$, $\sigma(T) \subset T$.

Thus T is a normal extension of F if and only if for all $t \in T$ and $\sigma \in G(K,F)$, $\sigma(t) \in T$. Assume T is a normal extension of F. Let $\sigma \in G(K,F)$ and $\tau \in G(K,T)$. Then $\tau(\sigma(t)) = \sigma(t)$ for all $t \in T$ since $\sigma(t) \in T$. Now, $\sigma^{-1}(\tau(\sigma(t))) = \sigma^{-1}(\sigma(t)) = t$ for all $t \in T$. Then $\sigma^{-1}\tau\sigma \in G(K,T)$. Hence by definition of normal, $G(K,T)$ is a normal subgroup of $G(K,F)$.

Conversely, assume $G(K,T)$ is normal in $G(K,F)$. Then $\sigma^{-1}\tau\sigma$ is in $G(K,T)$. Hence for all $t \in T$, $\sigma^{-1}\tau\sigma(t) = t$. Then

$$\sigma(t) = \sigma(\sigma^{-1}\tau\sigma(t)) = \sigma\sigma^{-1}(\tau\sigma(t)) = \tau(\sigma(t)).$$

But then $\sigma(t) \in T$ for all $t \in T$. Thus $\sigma(T) \subset T$. Therefore, T is a normal extension of F if and only if $G(K,T)$ is normal in $G(K,F)$.

(5) Let T be a normal extension of F and let $\sigma \in G(K,F)$. since $\sigma(T) \subset T$, by (4), σ induces an automorphism $\bar{\sigma}$ of T such that $\bar{\sigma}(t) = \sigma(t)$ for all $t \in T$. Then $\bar{\sigma}$ must leave every element of F fixed. Hence $\bar{\sigma} \in G(K,F)$. Define a map ϕ: $G(K,F) \to G(T,F)$ by $\phi(\sigma) = \bar{\sigma}$ for all $\sigma \in G(K,F)$.

Let σ, $\tau \in G(K,F)$. Let $\bar{\sigma}$, $\bar{\tau} \in G(T,F)$ be induced by σ, τ. Now for all $t \in T$, $\overline{\sigma\tau}(t) = \sigma\tau(t) = \sigma(\tau(t))$ and $\bar{\sigma}\bar{\tau}(t) = \bar{\sigma}(\bar{\tau}(t)) = \bar{\sigma}(\tau(t)) = \sigma(\tau(t))$ since, by (4), $\sigma(t) \in T$. Then $\overline{\sigma\tau} = \bar{\sigma}\bar{\tau}$. Hence $\phi(\sigma\tau)(t) = \phi(\sigma\tau(t)) = \overline{\sigma\tau}(t) = \bar{\sigma}\bar{\tau}(t) = \phi(\sigma)\phi(\tau)(t)$. Thus ϕ is a homomorphism.

The kernel of ϕ is the set of $\sigma \in G(K,F)$ such that $\phi(\sigma)$ is the identity map in $G(T,F)$. But the identity map in $G(T,F)$ is $\bar{\sigma}$. Thus the kernel is the set of all $\sigma \in G(K,F)$ such that for all $t \in T$, $\phi(\sigma)(t) = \bar{\sigma}(t) = \sigma(t) = t$. But this is precisely $G(K,T)$ since T remains fixed. Thus the kernel of ϕ is $G(K,T)$.

Now, by the First Isomorphism Theorem, the image of $G(K,F)$ in $G(T,F)$ under ϕ is isomorphic to $G(K,F)/G(K,T)$. But the order of the image is the index of $G(K,T)$ in $G(K,F)$, which is $o(G(K,F))/o(G(K,T))$ since $G(K,F)$ is finite. By part (3), $o(G(K,F))/o(G(K,T)) = [T:F]$ and by 4.12, $[T:F] = o(G(T,F))$. Thus the image of $G(K,F)$ in $G(T,F)$ must be $G(T,F)$, and hence ϕ is onto. Thus $G(K,F)/G(K,T)$ is isomorphic to $G(T,F)$.

<u>5.4 EXAMPLE</u>. Consider the polynomial $p(x) = x^4 - 2$ over $\mathcal{Q}$. In the field of complex numbers $p(x)$ factors into

$$(x - u)(x + u)(x - iu)(x + iu),$$

where $u = \sqrt{2}$ and $i = \sqrt{-1}$. Then the splitting field of $p(x)$ over $\mathcal{Q}$ is $\mathcal{Q}(iu,u)$. But $\mathcal{Q}(iu,u) = \mathcal{Q}(i,u)$ since any element in $\mathcal{Q}(iu,u)$ is of the form

$$b_1 + b_2iu + b_3(iu)^2 + b_4(iu)^3 + b_5u + b_6(iu)u + b_7(iu)^2u + b_8(iu)^3u$$
$$= b_1 + b_2iu - b_3u^2 - b_4iu^3 + b_5u + b_6iu^2 - b_7u^3 - b_8i,$$

where $b_i \in \mathcal{Q}$, and any element in $\mathcal{Q}(i,u)$ is of the form

$$c_1 + c_2u + c_3u^2 + c_4u^3 + c_5i + c_6iu + c_7iu^2 + c_8iu^3,$$

where $c_i \in \mathcal{Q}$.

By 2.5, $[\mathcal{Q}(iu):\mathcal{Q}] = [\mathcal{Q}(i,u):\mathcal{Q}(u)][\mathcal{Q}(u):\mathcal{Q}]$. Any element of $\mathcal{Q}(i,u)$ over $\mathcal{Q}(u)$ is of the form $c_1 + c_2i$ where c_1, $c_2 \in \mathcal{Q}(u)$.

Then $\{1,i\}$ is a basis for $\mathcal{Q}(i,u)$ over $\mathcal{Q}(u)$, and hence, by 2.11, $[\mathcal{Q}(i,u):\mathcal{Q}(u)] = 2$. Similarly, any element of $\mathcal{Q}(u)$ over $\mathcal{Q}$ is of the form $c_1 + c_2u + c_3u^2 + c_4u^3$, where $c_i \in \mathcal{Q}$. Hence a basis for $\mathcal{Q}(u)$ over $\mathcal{Q}$ is $\{i,u, u^2, u^3\}$ and $[\mathcal{Q}(u):\mathcal{Q}] = 4$. Thus $[\mathcal{Q}(i,u):\mathcal{Q}] = 8$. Then the group of automorphisms of $\mathcal{Q}(i,u)$ has eight elements. Let I be the identity map, $\sigma(u,i) \to (iu,i)$, and $\tau(u,i) \to (u,-1)$. All of the automorphisms can be expressed in terms of the generators σ and τ, by means of the equations $\sigma^4 = I$, $\tau^2 = I$, and $\tau\sigma = \sigma^3\tau$. Then

$I(u,i) \to (u,i)$

$\sigma(u,i) \to (iu,i)$

$\sigma^2(u,i) \to (-u,i)$

$\sigma^3(u,i) \to (-ui,i)$

$\tau(u,i) \to (u,-i)$

$\sigma\tau(u,i) \to (iu,-i)$

$\sigma^2\tau(u,i) \to (-u,-i)$

$\sigma^3\tau(u,i) \to (-iu,-i)$

The subgroups of the group of automorphisms of $\mathcal{Q}(i,u)$ are classified by order, with their corresponding fixed fields as follows:

Order 8	G_1 = the whole group	$F_1 = \mathcal{Q}$
Order 4	$G_2 = \{I, \sigma, \sigma^2, \sigma^3\}$	$F_2 = \mathcal{Q}(i)$
	$G_3 = \{I, \sigma^2, \tau, \sigma^2\tau\}$	$F_3 = \mathcal{Q}(u^2)$
	$G_4 = \{I, \sigma^2, \sigma\tau, \sigma^3\tau\}$	$F_4 = \mathcal{Q}(iu^2)$
Order 2	$G_5 = \{I, \sigma^2\}$	$F_5 = \mathcal{Q}(i,u^2)$
	$G_6 = \{I, \tau\}$	$F_6 = \mathcal{Q}(u)$
	$G_7 = \{I, \sigma\tau\}$	$F_7 = \mathcal{Q}(u(1 + i))$

	$G_8 = \{I, \sigma^2\tau\}$	$F_8 = \mathcal{Q}(iu)$
	$G_9 = \{I, \sigma^3\tau\}$	$F_9 = \mathcal{Q}(u(1 - i))$
Order 1	$G_{10} = \{I\}$	$F_{10} = \mathcal{Q}(i,u)$

Hence the Galois group of $p(x)$ over $\mathcal{Q}$ is G_1. Each subgroup of G_1 corresponds to a subfield of $\mathcal{Q}(i,u)$, which is its field, by the Fundamental Theorem.

For example, consider the subgroup G_7. The fixed field of this group is the set of elements left fixed by I and $\sigma\tau$. Clearly I leaves every element fixed. Now, for $\theta \in \mathcal{Q}(i,u)$,

$$\theta = c_1 + c_2u + c_3u^2 + c_4u^3 + c_5i + c_6iu + c_7iu^2 + c_8iu^3,$$

where $c_i \in \mathcal{Q}$. Then

$$\sigma\tau(\theta) = c_1 + c_2iu - c_3u^2 - c_4iu^3 - c_5i + c_6u + c_7iu^2 - c_8u^3.$$

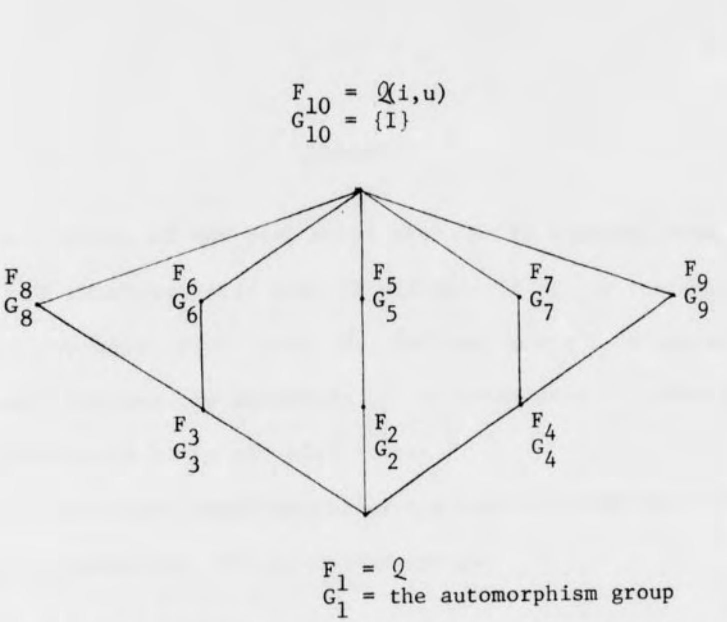
If $\sigma\tau(\theta) = \theta$, then $c_2 = c_6$, $c_3 = c_5 = 0$, $c_4 = -c_8$, and c_1, c_7 are arbirtary. Thus

$$\begin{aligned}\theta &= c_1 + c_2u + c_4u^3 + c_2iu + c_7iu^2 - c_4iu^3\\ &= c_1 + c_2u(1 + i) + c_7iu^2 + c_4u^3(1 - i)\\ &= c_1 + c_2u(1 + i) + (c_7/2)(u(1 + i))^2 - (c_4/2)(u(1 + i))^3.\end{aligned}$$

Hence $\mathcal{Q}(u(1 + i))$ is the fixed field of G_7.

The diagram on page 46 illustrates the correspondence of the subfields and the subgroups. [2]

The following discussion illustrates parts of the Fundamental Theorem. (1) Consider the subfield $\mathcal{Q}(u)$ of $\mathcal{Q}(i,u)$. Then the group of automorphisms of $\mathcal{Q}(i,u)$ relative to $\mathcal{Q}(u)$ consists of I and τ, which is just G_6. The fixed field of G_6 is $F_6 = \mathcal{Q}(u)$. Hence $\mathcal{Q}(i,u)$ is a normal extension of $\mathcal{Q}(u)$.



(2) Now look at the subgroup G_2 of G_1. The fixed field of G_2 is $F_2 = \mathcal{Q}(i)$. The automorphisms of $\mathcal{Q}(i,u)$ which leave $\mathcal{Q}(i)$ fixed are I, σ, σ^2, σ^3. But this is just G_2. Hence G_2 is closed.

(3) Now, $[\mathcal{Q}(i,u):\mathcal{Q}] = 2$, from the first part of this example, and $o(G_6) = 2$. Thus $[\mathcal{Q}(i,u):\mathcal{Q}(u)] = o(G_6) = o(G(\mathcal{Q}(i,u),\mathcal{Q}(u)))$. Also from this example, $[\mathcal{Q}(u):\mathcal{Q}] = 4$ and the order of the Galois group of $\mathcal{Q}(i,u)$ relative to $\mathcal{Q}$ is $o(G_1) = 8$. Hence,

$$O(G(\mathcal{Q}(i,u),\mathcal{Q}))/o(G(\mathcal{Q}(i,u),\mathcal{Q}(u))) = o(G_1)/o(G_6) = 4 = [\mathcal{Q}(u):\mathcal{Q}].$$

SUMMARY

In conclusion, it has been shown that K is a normal extension of a field F of characteristic zero if and only if K is the splitting field of a polynomial $p(x)$ over F. Further, there is a one-to-one correspondence between the subfields of K containing F onto the subgroups of the Galois group of $p(x)$ over F.

These results on field extensions are used to study the roots of polynomials by examining the associated groups.

BIBLIOGRAPHY

1. Emil Artin, Galois Theory, edited by Arthur N. Milgram, 2nd. ed., Notre Dame, Indiana, 1959.

2. Emil Artin, Modern Higher Algebra: Galois Theory, notes by Albert A. Blank, Courant Institute of Mathematical Sciences, New York University, New York, 1947.

3. John Fraleigh, A First Course in Abstract Algebra, Addison-Wesley, Reading, Massachusetts, 1967.

4. Lisl Gaal, Classical Galois Theory With Examples, Markham Publishing Company, Chicago, 1971.

5. I. N. Herstein, Topics in Algebra, Blaisdell Publishing Company, Waltham, Massachusetts, 1964.

6. Irving Kaplansky, Fields and Rings, University of Chicago Press, Chicago, 1969.

7. Seth Warner, Modern Algebra, vol. 2, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1965.