AN ABSTRACT OF THE THESIS OF

Richard Allan Laird for the Masters of Science

in Mathematics presented on April 28,1989

Title: Fundamentals of Galois Theory

Abstract Approved: Essam Abdelkeen

Galois Theory gives a necessary and sufficient condition for the solvability of polynomials by the elementary arithmatic operations and extraction of roots. The problems of trisecting angles and constructing polynomials with a specific number of sides are also answered in the field of Galois Theory. The purpose of this thesis is to establish the Fundamental Theorem of Galois Theory. This theorem shows the existence of a one-to-one correspondence, that reverses inclusion, between the subfields of a finite normal separable extension of a base field of characteristic zero and the subgroups of the automorphism group of the extension field which fix the base field. We also examine the concepts of algebraic extensions and splitting fields of irreducible polynomials.

FUNDAMENTALS OF GALOIS THEORY

A Thesis

Presented to

The Division of Mathematical and Physical Sciences

EMPORIA STATE UNIVERSITY

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

By

Richard A. Laird

April, 1989

Essam Abattein

Approved for the Major Division

James G. Anderson

Committee Member

Glenn A. Adamson

Committee Member

Essam Abattein

Committee Chairman

James L Wolfe

Approved for the Graduate Council

ACKNOWLEDGEMENT

I would like to thank Dr. Essam Abotteen for his help and patience, without either of which this paper would not have been possible. I would also like to thank Dr. John Carlson, the former head of the Math and Physical Science Department, for encouraging me to come back to school and giving me the financial support to allow me to do so. Special thanks to Dr. Stephanos Gialamas, a former faculty member, for helping me to believe in myself. Thanks to the entire Math Department at Emporia State University for putting up with me for so long. Thanks to my fiance, Janet Sharp for feeding me when I forgot and calming me down when I got too excited, and for loving me. But above all I would like to thank my father, Professor Emeritus Lester Laird for his encouragement and a few well-placed kicks that kept me moving.

CHAPTER 1

Introduction

The rational number field does not contain the solution to $x^2 - 2 = 0$; the angle $\frac{\pi}{3}$ cannot be trisected by a straight edge and compass; the polynomial equation $x^5 - 4x + 2 = 0$ cannot be solved by the elementary arithmetic operations and extraction of roots; and a polygon of 17 sides can be contructed with a straight edge and compass. These seemingly unrelated problems all have a common bond in the field of mathematics known as Galois Theory.

Evariste Galois (1811-1832) was able to establish a necessary and sufficient condition for the solvability of a polynomial equation by radicals. He associated a group with each polynomial, and proved that a polynomial equation could be solved by radicals if and only if the associated group is a solvable group. This was the first use of the word "group" in mathematical literature. Earlier, Abel (1802-1829) had proved that fifth degree and higher polynomials could not be solved by radicals in the general case

Galois's road to mathematical greatness was characterized by many detours. That he was able to accomplish anything at all was a tribute to his mathematical ability. His ability was not readily apparent when he first started school. Most of his early school teachers considered him a dim-witted troublemaker with no aptitude for mathematics.

He cared little for his classwork, and his work remained mediocre. Had his teachers known their dim-witted young student was too busy reading Legrendre's *Geometry* to bother with the routine classwork they would have surely changed their opinions of him. His ability to comprehend not only Legrendre's work, but later the works of Lagrange and Cauchy led young Galois to attempt admission to L'École Polytechnique, the premier mathematical school of France. It was there he hit his first pothole, as he was denied entrance due to his lack of formal training. This did not stop him from his mathematical work and at the age of seventeen he submitted a paper to Cauchy which was to be presented to the Académie des Sciences. Cauchy already had one temporarily misplaced paper from Abel to his credit, but he outdid this deed by completely losing Galois's paper. Galois now had not only the examiners from L'École Polytechnique erecting barricades to his progress, but the academicians as well. A second attempt to gain admission to the school also ended in rejection. As if these events were insufficient to fuel Galois's hatred of authority, he received news of his father's death. Galois's father was the mayor of the town where Galois grew up and a staunch opponent of the clergy. False rumors spread by a priest had caused the older Galois to lose his job and in despair, his father commited suicide.

Galois made no more attempts to gain entrance to L'École Polytechnique, and settled for L'École Normale, where he went into training to become a teacher. He did not stop his research in mathematics however, and in 1830 submitted a paper to the Académie in competition for its prize in mathematics This time Fourier had the honor of losing Galois's paper, although he had to die to do it. By now Galois was a very bitter young man and threw his efforts into the revolution then occuring in France. By way of a letter denouncing the administration of L'École Normale, he managed to get expelled from the school. He still continued his mathematical writings and submitted another paper to the Académie, this time through Poisson. Poisson, at least, did not lose the paper, what he did do was find it "incomprehensible" and returned it to Galois This paper contained some of the important results of the field of study that now bears Galois's name. Galois did not attempt to submit any more papers to be presented to the Académie. Instead Galois became a leader of the revolution. His popularity with the people probably saved him from worse treatment than he received at the hands of the authorities. As it was he was arrested twice and the second time spent six months in jail. Shortly after his release he was challenged to a duel. It is not clear whether it was over a woman or his political activities, only that he did not survive it. The night before the duel

he stayed up writing a letter in which he attempted to set down his mathematical ideas. Galois had intended his posthumus letter and manuscripts for the Académie, but they ended up with Liouville. They were edited and published in his *Journal* in 1846, fourteen years after Galois's death.

Galois Theory has roots that go back at least as far as 1700 B.C., for the Babylonians had a method of solving quadratic equations. We do not know how the Babylonians came up with their version of the quadratic formula, or whether they understood why it worked or if they merely followed a recipe that gave correct answers. The Babylonians did not possess knowledge of negative numbers, so they had a couple of versions of the process to deal with sums and differences. In modern algebraic terms, they wanted to find solutions to $x + y = s$ and $xy = p$, where s and p are given numbers. The steps the Babylonians used are:

1) Take half of s

2) Square the result

3) From this subtract p

4) Take the square root of the result

5) To this, add one half of s for one of the numbers; then subtract this number from s to get the other number.

In symbolic form: $x = \sqrt{\left(\frac{s}{2}\right)^2 - p} + \frac{s}{2}$, and $y = x - s$. In other words, the Babylonians knew how to complete the square

It was not until the 15th century during the Italian Renaissance that any major progress was made in the field of algebra, the Ancient Greeks had worked mainly in geometry. For mathematics, the Renaissance was not a rebirth, but a period of new growth. In the sixteenth century an algebraic solution of cubic equations was discovered. The Arabs had solved the cubic, but as points of intersection of conic sections, not by any algebraic methods. In 1545 Geronimo Cardano (1501-1576) of Italy published both the solution to the cubic and to the quartic equations. For this reason the year 1545 is frequently taken as the beginning of the modern era of mathematics. Cardano was not the originator of the discovery, he having obtained a hint, through bribery and fraud, for solving the cubic from Niccolo Tartaglia (ca. 1500-1557). Cardano had promised not to reveal the solution since he knew Tartaglia planned to make his reputation by publishing it. Tartaglia himself had a habit of publishing material that was not his own without giving credit to the originators, so little sympathy is due him; at least Cardano gave credit to Tartaglia in his publication. There is also evidence that Tartaglia had received a hint for solving the problem from a third source, ample evidence that plagarism and intellectual theft have a long history. The credit for being the first to solve the cubic is generally given to Scipione del Ferro (ca. 1465-1526) who did not publish his findings.

The solution of the quartic equation was accomplished by a student of Cardano's, Ludovico Ferrari. Again, since they did not use negative numbers, they had twenty separate cases to consider. His method was to reduce the quartic equation to a cubic, known today as the "resolvent cubic", which could then be solved by methods already known.

Finding the general solutions to the cubic and quartic equations were the first real advances made in the theory of equations since the time of the Babylonians. However, we should emphasize that these were only an advance in theoretical mathematics. Approximate solutions to some cubics were known in antiquity. For example, al-Kashi (ca 1436) could find an approximate solution to any cubic equation to any desired degree of accuracy. So these theoretical discoveries did not help in the solution of any practical problems. What they did do was to cause a lot of mathematical attention to be focused on the field of algebra. It was only logical that mathematicians would attempt to extend the methods of solving the cubic and quartic equations to solving the quintic equation. This problem was to occupy mathematicians for the next couple of centuries as they were faced with an unsolved algebraic problem comparable to the classical geometric problems of the Greeks.

The eighteenth century in France was a time of great turmoil and of great mathematical discoveries. This was the time of Lagrange, Laplace, Legrendre, Carnot, Condorcet, and Monge. It had the misfortune to fall between the seventeenth (The Century of Genius) and nineteenth (The Golden Age) centuries. Much of what was discovered during the eighteenth century pointed the direction for what was to follow. This is especially true for the topic of this paper. In 1770 Lagrange published a paper where he considered the solvability of equations in terms of permutations of their roots It was to the works of Lagrange, Legendre, and Cauchy that the fifteen year old Galois turned when disgusted with the algebra texts his boarding school provided.

To summerize, Galois's work was published posthumously by Liouville in 1846 in his *Journal*. Abel (1802-1829) had already shown the fifth degree polynomial was unsolvable by radicals. Galois was able to show that a polynomial equation was solvable by radicals if and only if the symmetric group on its roots is a solvable group. Although Galois Theory provides an algorithm for finding the roots of a polynomial that is solvable by radicals, the main thrust of Galois Theory is the algebraic structures of the systems arising from the polynomials. It was the ideas of Galois that led to the careful postulational treatment of

algebraic structures. Galois and Abel had the concept of fields implicit in their work, but the explicit definition of a number field did not occur until 1879 by Dedekind (1831-1916). This led to the ideas of integral domains, a generalization of the idea of the integers. As described the search for the solution to the problem of solving polynomials of any degree has led to many important discoveries.

In this paper we are mainly concerned with establishing the Fundamental Theorem of Galois Theory for finite, normal, separable field extensions. The proof that fifth degree and higher polynomials cannot be solved by radicals, while probably the most famous result of Galois, is beyond the scope of this study. In Chapter 2 we will present some background information on ring theory in a form designed for the material developed in the later chapters on field extensions. This is the subject of Chapter 3 and the main body of work in the paper. In it we will examine finite field extensions, algebraic extensions, splitting fields for polynomials and the concept of normal extensions, and finally separable extensions. Chapter 4 is the Fundamental Theorem of Galois Theory, where we show there is a one-to-one correspondence between the intermediate fields of a finite normal separable field extension and the subgroups of the Galois group of the field extension.

CHAPTER 2

Rings and Ideals

This chapter will present some ideas, definitions, and theorems which will be useful in the following chapters.

Def 2.1: A ring is a triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are binary operations on R. $(R, +)$ is a Abelian Group and $(R, \cdot)$ is a semi-group and the operations are related by the distributive laws;

1) $a(b + c) = ab + ac$

2) $(a + b)c = ac + bc$.

If $ab = ba$ for all $a, b \in R$, then R is a commutative ring. If there exists an element e of R, such that $ae = ea = a$ for all $a \in R$, then R is a ring with unity. In what follows e will be denoted by 1.

Examples: $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$, $(\mathbf{C}, +, \cdot)$, $(\mathbf{Z}_n, +, \cdot)$ are all examples of commutative rings with identities with respect to multiplication.

Homomorphisms and isomorphisms between rings are logical extensions of the same concepts for groups.

Def 2.2: A ring homomorphism between two rings R and R' is a mapping $\phi: R \to R'$ where, for all $a, b \in R$;

1) $\phi(a + b) = \phi(a) + \phi(b)$

2) $\phi(ab) = \phi(a)\phi(b)$.

If R and R' are rings with unities 1 and 1' respectively, then we require $\phi(1) = 1'$.

Def 2.3: If ϕ is a ring homomorphism and ϕ is 1-1, then ϕ is a ring isomorphism.

Def 2.4: Two rings R and R' are said to be isomorphic iff there exists an isomorphism ϕ from R to R' and ϕ is onto. This will be denoted $R \simeq R'$.

Def 2.5: A subring of R is a subset S, of R, which is a ring itself with respect to the same binary operations as R.

Examples. $\mathbf{Z}$ is a subring of $\mathbf{Q}$, $\mathbf{R}$, and $\mathbb{C}$; $\mathbf{Q}$ is a subring of $\mathbf{R}$ and $\mathbb{C}$, $\mathbf{R}$ is a subring of $\mathbb{C}$.

Thm 2.1: Let S be a non-empty subset of a ring R, then S is a subring of R iff for all a, b $\in$ S, we have $a - b \in S$ and $ab \in S$.

Example: The set $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} \ / \ m, n \in \mathbf{Z}\}$ is a subring of the ring of real numbers.

Def 2.6: A commutative ring $(R, +, \cdot)$ is an integral domain iff whenever $ab = 0$, then either $a = 0$ or $b = 0$.

Remark: If $a \neq 0 \in R$ and there exists $b \neq 0 \in R$ and $ab = 0$ then a and b are zero divisors. So an integral domain is a commutative ring with no zero divisors.

Def 2.7: If $a \in R$ and there exists $b \in R$ such that $ab = 1$, then a is a unit of R.

If every non-zero element of R is a unit, then we have the group structure on $R - \{0\}$ under the operation of multiplication.

Def 2.8. A ring $(R,+,\cdot)$ is a division ring iff $(R - \{0\},\cdot)$ is a group.

To get to the field structure we must require the multiplicative group to be commutative.

Def 2.9: A ring $(R, +, \cdot)$ is a field iff $(R - \{0\}, \cdot)$ is an Abelian group.

Def 2.10: Let $(R, +, \cdot)$ be a ring and C be the set:

$$C = \{ n \in \mathbb{Z}^+ \ / \ nr = 0 \text{ for all } r \in R \}.$$

If $C = \emptyset$ then R is said to have characteristic zero. If $C \neq \emptyset$ then the smallest number in C is the characteristic of R. The definition for the characteristic of a field is

the same as for a ring.

Examples: 1) Let R be the ring of integers, $\mathbf{Z}$. Since there does not exist an $n \in \mathbf{Z}^+$ such that $1n = 0$, $\mathbf{Z}$ has characteristic zero.

2) Consider $\mathbf{Z}_3$. C will be the set $\{3, 6, 9, 12, \ldots\}$ since $3k(z) \equiv 0$ for all $k \in \mathbf{Z}^+$ and for all $z \in \mathbf{Z}_3$. So the characteristic of $\mathbf{Z}_3$ is 3. In fact, for any n, $\mathbf{Z}_n$ will have characteristic n.

Def 2.11: Let $(R, +, \cdot)$ be a ring. A non-empty subset A of R is a two-sided ideal of R iff:

1) $a_1 - a_2 \in A$ for all $a_1, a_2 \in A$

2) If $a \in A$, then $ra \in A$ and $ar \in A$ for all $r \in R$.

Let R be a ring and I an ideal of R. Let $\frac{R}{I}$ be the set of all the distinct cosets of I in R obtained by considering I as a subgroup of R under addition, i.e $\frac{R}{I} = (a + I \;/\; a \in R)$. We know $\frac{R}{I}$ is an abelian group under the addition of cosets which is defined by;

$$(a + I) + (b + I) = (a + b) + I$$

Similarly if we define multiplication in $\frac{R}{I}$ by;

$$(a + I)(b + I) = (ab + I)$$

One can prove this is a well-defined binary operation and $\frac{R}{I}$, with respect to these operations, is a ring and it will be called the quotient ring of R with respect to the ideal

I.

Thm 2.2: Let ϕ: R $\rightarrow$ S be a ring homomorphism between ring R and S, then:

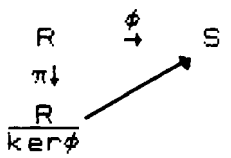
1) ker ϕ is an ideal of R,

2) ϕ is an isomorphism iff ker ϕ = (0),

3) If U is a subring or ideal of R, then ϕ(U) is a subring or ideal of S,

4) If T is a subring of S, then ϕ^{-1}(T) is a subring of R, moreover if T is an ideal of S, then ϕ^{-1}(T) is an ideal of S.

Thm 2.3: (Fundamental Theorem of Ring Homomorphisms) Let ϕ: R $\rightarrow$ S be a ring homomorphism. Then there exists a unique ring isomorphism $\bar{\phi}$: $\frac{R}{\ker \phi} \rightarrow$ S such that the following diagram commutes.



In particular $\phi(R) \simeq \frac{R}{\ker\phi}$ Here π is the canonical homomorphism π: R $\rightarrow \frac{R}{\ker\phi}$, given by $\pi(a) = a + \ker \phi$.

Def 2.12: An ideal P is a proper ideal of a ring R iff P $\neq$ R or P $\neq$ (0).

In a non-commutative ring we must differentiate between

left ideals and right ideals, but in this paper we will be dealing with commutative rings, so all rings can be assumed to be commutative unless otherwise specified. Now we want to look at an ideal that is generated by a subset of a ring. Let S be an arbitrary subset of a ring R. The set of elements of the form $\sum r_i s_{ij}$, $r_i \in R$ and $s_{ij} \in S$ and of finite length form an ideal. It is called the ideal generated by S. If $S = \{s_1, s_2, \ldots, s_n\}$ then the ideal generated by S is denoted $\langle\{s_1, s_2, \ldots, s_n\}\rangle$ The elements of S are called the generators of the ideal.

Def 2.13: An ideal that is generated by a single element is known as a principal ideal.

Def 2.14: Let R be a commutative ring. An ideal $P \neq R$ is a prime ideal iff whenever $ab \in P$ then either $a \in P$ or $b \in P$.

Def 2.15: An ideal M is a maximal ideal of a ring R iff $M \neq R$ and if U is an ideal of R where $M \subseteq U \subseteq R$, then either $U = M$ or $U = R$.

Given a ring R there is no guarantee that it has any maximal ideals. However if R has a unit element then it has a maximal ideal (the Axiom of Choice is needed to prove this). Also there may be more than one maximal ideal in a

ring R.

Example: Let R = $\mathbf{Z}$ and let p be a prime, then I = p$\mathbf{Z}$ is a maximal ideal.

Thm 2.4: If R is a commutative ring with unity, and M is an ideal of R, then M is a maximal ideal of R iff $\frac{R}{M}$ is a field.

Corollary 2.1: A commutative ring with unity is a field iff it has no proper non-trivial ideals.

Thm 2.5: Let R be a commutative ring with unity, and let P $\neq$ R be an ideal in R. Then P is a prime ideal iff $\frac{R}{P}$ is an integral domain.

Since every field is an integral domain, we have the following corollary.

Corollary 2.2: Every maximal ideal in a commutative ring R with unity is a prime ideal.

Def 2.16: A field P is a prime field iff it has no subfield other than itself.

Example: 1) $\mathbf{Q}$ is a prime field. If E $\subseteq$ $\mathbf{Q}$ then $\mathbf{Z}$ $\subseteq$ E so

$\frac{1}{n} \in E$ for all $n \in \mathbf{Z}$, $n \neq 0$ and $\frac{m}{n} \in E$ for all $m \in \mathbf{Z}$, so $E = \mathbf{Q}$.

2) $\mathbf{Z}_p$ is a prime field.

$$\mathbf{Z}_p = \frac{\mathbf{Z}}{\langle p \rangle} = \left\{ n + p\mathbf{Z} \;/\; n \in \mathbf{Z} \text{ and } p \text{ is a prime} \right\}.$$

$E \subseteq \mathbf{Z}_p \Rightarrow 1 + p\mathbf{Z} \in E$ but,

$n + p\mathbf{Z} = n\,(1 + p\mathbf{Z})$ so $n + p\mathbf{Z} \in E$ and $E = \mathbf{Z}_p$.

Thm 2.6: A field F of characteristic 0 is prime iff $F \simeq \mathbf{Q}$. A finite field F of characteristic p is prime iff $F \simeq \mathbf{Z}_p$ for some prime p.

Polynomial Rings

Let R be a ring Define the set $P(R) = \{(a_0, \ldots, a_n \;)/ a_i \in R, i \in \mathbf{Z}^+$ and a finite number of the a_i's are not zero$\}$. Let $a = (a_0, \ldots, a_n, \ldots)$ and $b = (b_0, \ldots, b_n, \ldots)$. Define $a = b$ iff $a_i = b_i$ for all $i \in \mathbf{Z}^+$. Addition can be defined on P(R) by $c = a + b = (a_0 + b_0, \ldots, a_n + b_n, \ldots)$, i. e., $c_i = a_i + b_i$. Clearly $c \in P(R)$. Multiplication can be defined on P(R) by $c = ab$; where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. Again $c \in P(R)$. P(R) is called a polynomial ring over R. P(R) is commutative iff R is commutative and P(R) has unity iff R has unity. $(1_R, 0, 0, \ldots)$ is unity for P(R). We can define a mapping ϕ: $R \to P(R)$ by $\phi(r) = r' = (r, 0, 0, \ldots)$, then $R \simeq \phi(R)$. So we can think of R as a subring of P(R) under the identification $r \mapsto (r, 0, 0, \ldots)$.

Let R be a ring with unity 1. Define $x = (0, 1, 0, \ldots)$, then

$x^2 = (0, 0, 1, 0, \ldots)$

$x^3 = (0, 0, 0, 1, 0, \ldots)$

$\vdots$

$x^n = (0, 0, \ldots, 1, \ldots)$ where the 1 is in the $n + 1$ place. Then

$a_1x = (0, a_1, 0, \ldots)$

$a_2x^2 = (0, 0, a_2, 0, \ldots)$, etc.

Hence an element $a \in P(R)$ can be written as $a = (a_0, a_1, \ldots) = a_0 + a_1x + a_2x^2 + \ldots$. We call x an indeterminate and the a_i's coefficients. In the remainder of the paper the polynomial ring P(R) will be denoted R[x]. An element $f(x) \in R[x]$ will be denoted by $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$. The degree of f(x) is the largest value of n for which a_n is not zero and will be denoted by $\deg(f(x)) = n$. The zero polynomial is the polynomial with all the a_i's equal to zero and it's degree shall be the symbol $-\infty$ and we will adopt the usual conventions that, $-\infty < n$ for every n, $(-\infty) + (-\infty) = -\infty$, $-\infty + n = -\infty$. If $f(x) = a_0 + a_1x + a_2x^2 + \ldots a_nx^n$ and $\deg(f(x)) = n$, then a_n is called the leading coefficient of f(x).

Thm 2.7: If $f, g \in R[x]$, where R is a ring with 1, then

1) $\deg(f + g) = \max\{\deg f, \deg g\}$, and

2) $\deg(fg) \leq \deg f + \deg g$.

The equality in (2) will hold if R has no zero divisors. In particular the equality holds in a polynomial ring over an integral domain.

A constant polynomial is one where a_i equals zero for all $i \geq 1$. We should note here that the degree of a non-zero constant polynomial is 0. The only units of R[x] are the constant polynomials which correspond to the units in R under the embedding $r \rightarrow (r, 0, 0, \ldots)$.

Thm 2.8: (Division Algorithm) Let R be a commutative ring with unity and $f(x)$, $g(x) \in R[x]$. If $g(x)$ has a leading coefficient b, then there exists a non-negative integer k and $q(x)$, $r(x) \in R[x]$ such that:

1) $b^k f(x) = q(x)g(x) + r(x)$ with $\deg(r(x)) < \deg(g(x))$

2) If b is not a zero divisor in R, then $q(x)$ and $r(x)$ are unique.

3) If b is a unit in R we may take $k = 0$.

In the following we will be concerned with polynomials over fields, in which case we have the following corollary.

Corollary 2.3: Let F be a field. For any polynomials $f(x)$, $g(x) \in F[x]$, there exists unique polynomials $q(x)$, $r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$ and

$\deg(r(x)) < \deg(g(x))$.

Corollary 2.4: (Remainder Theorem) Let F be a field. If $f(x) = a_0 + \ldots + a_n x^n \in F[x]$ and $a \in F[x]$, then there exists a unique polynomial $g(x) \in F[x]$ such that $f(x) = (x - a)g(x) + f(a)$, where:

$f(a) = a_0 + a_1 a + a_2 a^2 + \ldots + a_n a^n$, (i.e. f(a) is the value of f(x) at a in the classical sense).

Corollary 2.5: (Factor Theorem) Let F be a field. If $f(x) \in F[x]$ and $a \in F$, then $(x - a)$ is a factor of f(x) (in the sense that $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$) iff $f(a) = 0$.

Def 2.17: Let F be a field and $f(x) \in F[x]$. Any element $a \in F$ such that $f(a) = 0$ is called a zero of f(x) in F.

A consequence of the preceeding two corollaries is a limit on the number of zero that a polynomial can have.

Corollary 2.6: A non-zero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in F.

Our next definition singles out a type of polynomials in the polynomial ring F[x] that is of major importance in the remainder of the paper.

Def 2.18: Let F be a field. A non-constant polynomial $f(x) \in F[x]$ is said to be irreducible over F iff $f(x)$ cannot be expressed as the product of two polynomials $g(x), h(x) \in F[x]$ where $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$. If $f(x)$ is not irreducible it is called reducible over $F[x]$

A polynomial which is irreducible over one field may be reducible over a different field. $x^2 - 2$ is irreducible over the rationals, but is reducible over the reals. In other words, the irreducibility of a polynomial depends as much on the field in question as the polynomial itself.
In $F[x]$ the units are precisely the non-zero elements of F. therefore we could have defined an irreducible polynomial $f(x)$ in $F[x]$ as a non-constant polynomial where any factorization $f(x) = g(x)h(x)$, must result in either $g(x)$ or $h(x)$ being a unit in $F[x]$.

Numerous sufficient conditions for a polynomial to be irreducible are known. We will present only one of them here.

Eisenstein's criterion for irreducibility:
Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbf{Z}[x]$. If there exists a prime p such that $p|a_0, p|a_1, \ldots, p|a_{n-1}$, but $p\nmid a_n$ and $p^2\nmid a_0$, then $f(x)$ is irreducible in $\mathbf{Z}[x]$ and also is irreducible over $\mathbf{Q}$.

Example: Let $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$, and let $p = 3$, then $f(x)$ is irreducible over $\mathbf{Q}$.

Corollary 2.7: For any prime $p \in \mathbf{Z}$, the cyclotomic polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over $\mathbf{Q}$.

Eisenstien's criterion holds when $\mathbf{Z}$ is replaced with a unique factorization domain D and $\mathbf{Q}$ is replaced by the field of quotients of D.

Def 2.19: A commutative ring R is a principal ideal ring iff every ideal of R is a principal ideal. A principal ideal ring which is an integral domain is a principal ideal domain.

Example: $(\mathbf{Z}, +, \cdot)$ is a principal ideal domain.

Thm 2.9: If F is a field, F[x] is a principal ideal domain.

Thm 2.10: Let F be a field and let $p(x) \in F[x]$, $p(x) \neq 0$. The ideal $\langle p(x) \rangle$ is maximal iff $p(x)$ is irreducible over F.

Proof: Assume $\langle p(x) \rangle$ is maximal.

Assume $p(x)$ is not irreducible, then there exists $g(x)$, $r(x) \in F[x]$ with degrees less than the degree of $p(x)$ such that $p(x) = g(x)r(x)$. Consider $\langle g(x) \rangle$. Since $p(x) = g(x)r(x)$, any element in $\langle p(x) \rangle$ can be written as $p(x)q(x) = g(x)r(x)q(x)$, for $q(x) \in F[x]$, and so is in $\langle g(x) \rangle$. So $\langle p(x) \rangle \subseteq \langle g(x) \rangle$. We can assume $g(x)$ is irreducible over F, since if it isn't we can write it as the product of two polynomials with lesser degree and continue until we have an irreducible polynomial. $1 \notin \langle g(x) \rangle$. If it were, then $g(x)$ would be a constant polynomial and would have degree equal to zero. But then $\deg(p(x)) = \deg(r(x))$ which contradicts the definition of $r(x)$. Since $1 \notin \langle g(x) \rangle$, $\langle g(x) \rangle \neq F[x]$. This implies the degree of $g(x)$ equals the degree of $p(x)$, which contradicts the definition of $g(x)$. So $p(x)$ must be irreducible.

Assume $p(x)$ is irreducible.

Assume there exists an ideal I where $\langle p(x) \rangle \subset I \subset F[x]$. I is a principal ideal, so $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$. Since every element in $\langle g(x) \rangle$ is of the form $g(x)f(x)$, for some $f(x) \in F[x]$, the $\deg(g(x))$ is less than or equal to the degree of any other non-zero element of $\langle g(x) \rangle$. By the Division Algorithm there exists unique polynomials $q(x)$, $r(x) \in F[x]$ such that $p(x) = q(x)g(x) + r(x)$. So $r(x) \in \langle g(x) \rangle$. But since $\deg(r(x)) < \deg(g(x))$, $r(x)$ must be zero, which means $p(x) = q(x)g(x)$. But $p(x)$ is irreducible

so I does not exist and $\langle p(x) \rangle$ is maximal.

Corollary 2.8: If $p(x) \in F[x]$ is irreducible over F, then $\frac{F[x]}{\langle p(x) \rangle}$ is a field.

CHAPTER 3

Field Extensions

In this chapter we will be looking at finite field extensions, introducing the concepts of algebraic extensions, normal extensions, and separable extensions. It will lead to the Galois theory of finite, normal, separable field extensions.

Some books define a field K to be an extension of a field F if F is a subfield of K, however this would exclude the case where K contains a subfield that is isomorphic to F, but not necessarily equal to F. The following definition will allow that possibility.

Def 3.1: Let F be a field. An extension of F is a pair (K, i) where K is a field and i: F $\rightarrow$ K is a ring monomorphism (1-1). K:F will mean that K is an extension of F.

The field F is called a ground field with respect to K. If K is an extension field of F with respect to ring monomorphism i: F $\rightarrow$ K, then F is embedded as a subfield of K via the identification of a $\in$ F with i(a). For the sake of brevity unless i is specifically needed for purposes of clarity we will not list it and just consider F as a subfield of K.

Examples: 1) The field of real numbers is an extension of the field of rational numbers and the field of complex numbers is an extension of both real and rational numbers.

2) $\mathbb{Q}(\sqrt{2}) = \{ p + q\sqrt{2} \ / \ p, q \in \mathbb{Q} \}$ is an extension of $\mathbb{Q}$.

If we consider a field F and the family M_α, $\alpha \in I$, of all subfields of F, then the intersection M of all these subfields will be the prime field of F. But, as we will see in the next theorem, this prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p. So we can view every field F, as an extension of a field isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ depending on whether the characteristic of F is 0 or some prime p.

Thm 3.1: Let F be a field. The prime field of F is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$.

Proof: Let F be a field whose unity is denoted e and let $\mathbb{Z}$ be the ring of integers. Let Δ be the prime field of F.

Define ϕ: $\mathbb{Z} \to F$ by:

$$\phi(n) = ne, \text{ where } ne = \begin{cases} ne & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -(-n)e & \text{if } n < 0 \end{cases}$$

ϕ is a homomorphism from $\mathbb{Z}$ into F. Since $e \in \Delta$, ϕ maps $\mathbb{Z}$ into Δ. The kernal of ϕ is not all of $\mathbb{Z}$ since $\phi(1) = e \neq 0$. Suppose ϕ is an isomorphism. Then Δ has a subring isomorphic to $\mathbb{Z}$ and therefore a subfield isomorphic to the field of quotients of $\mathbb{Z}$, namely $\mathbb{Q}$. But since Δ is the smallest subfield of F, Δ is the subfield and $\Delta \simeq \mathbb{Q}$.

Suppose ϕ has a non-trivial kernal. This kernal is a principal ideal. Let $ab \in \ker \phi$, so $\phi(ab) = 0 \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$ since $\text{char}\mathbf{Z} = 0$. Assume $a = 0$, so $\phi(a) = 0$ and $a \in \ker \phi$. Ker ϕ is a prime ideal and $\frac{\mathbf{Z}}{\ker \phi}$ is an integral domain and ker ϕ is generated by a prime p. So Δ has a subring isomorphic to $\mathbf{Z}_p$. But $\mathbf{Z}_p$ is a field, so $\Delta \simeq \mathbf{Z}_p$.

Let K:F, then K can be considered as a vector space over F where addition is the usual addition in K and scalar multiplication is the usual field multiplication $a\alpha$, where $a \in F$ and $\alpha \in K$.

Def 3.2: The degree of the extension K:F is the dimension of K as a vector space over F. If $\dim_F(K)$ is finite then K:F is called a finite extension, and is infinite otherwise. The degree of K:F is denoted [K:F].

Lemma 3.1: $[K:F] = 1$ iff $K \simeq F$.

Thm 3.2: Let M:L and L:K, then [M:K] = [M:L][L:K].

Proof: We will prove this theorem by looking at the extension as a vector space over the base field. Let $\{\alpha_i / \ i \in I\}$ be a basis for M as a vector space over L and $\{\beta_j / \ j \in J\}$ be a basis for L as a vector space over K. We shall show $\{\alpha_i\beta_j / \ i \in I, \ j \in J\}$ is a basis for M as a vector

space over K.

First, to show linear independence assume $\sum_{i\in I}\sum_{j\in J}\gamma_{ij}\alpha_i\beta_j = 0$, where $\gamma_{ij} \in K$. This can be written $\sum_{i\in I}\left(\sum_{j\in J}\gamma_{ij}\beta_j\right)\alpha_i = 0$. Since $\sum_{j\in J}\gamma_{ij}\beta_j \in L$, $\forall\ i \in I$, $\sum_{j\in J}\gamma_{ij}\beta_j = 0$, $\forall\ i \in I$, and hence $\gamma_{ij} = 0$ for each $i \in I$ and $j \in J$, and we have linear independence. Then $\{\alpha_i / \ i \in I\}$ and $\{\beta_j / \ j \in J\}$ are bases for the respective vector spaces. Let $\delta \in M$, then $\delta=\sum_{i\in I}\eta_i\alpha_i$ where $\eta_i \in L$ and $i \in I$ and $\eta_i = \sum_{j\in J}\xi_{ij}\beta_j$ for $i \in I$ where $\xi_{ij} \in K$. Therefore $\delta = \sum_{i\in I}\sum_{j\in J}\xi_{ij}\beta_j\alpha_i$ and the $\alpha_i\beta_j$ span M over K.

Example: Looking at $\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}$, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}): \mathbb{Q}] = 4$

Corollary 3.1: [M:K] is finite iff [M:L] and [L:K] are finite.

Corollary 3.2: Let $F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_r$ be a sequence of subfields, then

$$[F_r:F_0] = [F_r:F_{r-1}][F_{r-1}:F_{r-2}] \cdots [F_1:F_0].$$

Corollary 3.3: If [K:F] = p, where p is a prime, then the only subfields of K are K and F.

Adjunction

In this section we will examine different types of

extensions and see how to construct them. We will be primarily concerned with finite extensions. The automorphisms of such extensions play an extremely important role in Galois theory.

Let K be a field and S a subset of K. Consider all subfields of K which contain S. The intersection of all these subfields is the smallest subfield of K which contains S. $\bigcap_{\substack{L\leq K \\ S\subseteq L}} L \leq K$

Def 3.3: Let K:F and let S be a subset of K. Let $Y = S \bigcup F$ and consider the intersection of all subfields of K which contain Y. $\bigcap_{\substack{L\leq K \\ Y\subseteq L}} L = F(S)$. This is the field obtained from F by adjoining S to F.

Remarks: 1) In general F(S) is larger than $F \bigcup S$

2) If a subfield F, of K, contains S, then it contains all polynomials in finitely many elements of S with coefficients in F and the quotients of such polynomials. Thus we have,

$$F(S) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(b_i, \ldots, b_m)} \Big/ \quad f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n], \right.$$
$$\left. g(x_1, \ldots, x_m) \in F[x_1, \ldots, x_m], \quad a_i, b_i \in S, \quad g(b_1, \ldots, b_m) \neq 0 \right\}$$

3) If $S = \{s_1, \ldots, s_n\}$ then $F(S) = F(\{s_1, \ldots, s_n\})$ will be denoted $F(s_1, \ldots, s_n)$. In particular $F(\{a\}) = F(a)$. From the definition of F(S), $S \subseteq F(S)$ and $F \leq F(S)$ and F(S)

is the smallest subfield of K that contains both F and S.

4) If S_1 and S_2 are subsets of K, then we have $F(S_1 \cup S_2) = (F(S_1))(S_2)$. Note that $F(S_1) \subseteq F(S_1 \cup S_2)$ and $F(S_2) \subseteq F(S_1 \cup S_2)$. Therefore $(F(S_1))(S_2) \subseteq F(S_1 \cup S_2)$. On the other hand $F \subseteq (F(S_1))(S_2)$ and $S_1 \cup S_2 \subseteq (F(S_1))(S_2)$. Therefore $F(S_1 \cup S_2) \subseteq (F(S_1))(S_2)$. Thus $F(S_1 \cup S_2) = (F(S_1))(S_2)$. We can therefore write $F(S_1, S_2)$ instead of $F(S_1 \cup S_2)$.

We will now define a special kind of field extension.

Def 3.4: Let K:F. K is a simple extension of F iff $K = F(a)$ for some $a \in K$.

It follows then, that any extension of F obtained by adjoining a finite set to F can be obtained by a sequence of simple extensions.

It is our objective to classify all possible simple extensions First we need to introduce the concept of isomorphism of extensions to classify all possible simple extensions up to isomorphism.

Def 3.5: Let $i: K \to K^*$ and $j: L \to L^*$ be field extensions. A field extension isomorphism between them is a pair of maps (ϕ, ϕ^*) where $\phi: K \to L$ and $\phi^*: K^* \to L^*$ are isomorphisms and $\phi^* \circ i = j \circ \phi$. That is, if the following diagram

comutes,

$$\begin{array}{ccc} K & \xrightarrow{i} & K^{\#} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi^{\#}} \\ L & \xrightarrow[j]{} & L^{\#} \end{array}$$

What this means is if the field structure is preserved by isomorphism $\phi : K \to L$ then the embedding of the smaller field in the larger one is also preserved by ϕ.

Def 3.6: Let K:F. An element $a \in K$ is called algebraic over F iff there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(a) = 0$. Otherwise a is transcendental over F.

Example: $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since $f(\sqrt{2}) = 0$ where $f(x) = x^2 - 2$. e and π are transcendental over $\mathbb{Q}$.

Def 3.7: F(a) is a simple algebraic extension of F iff a is algebraic over F. Otherwise F(a) is a simple transcendental extension of F.

We now want to look more closely at the structure of F(a). Let F[x] be the polynomial ring over F.

$$F[a] = \left\{ c_0 + c_1 a + \ldots + c_n a^n \;/\; c_i \in F,\ n \geq 0 \right\}$$

is an integral domain. It therefore has a quotient field that contains a and F, but F(a) is the smallest field which contains both a and F so F(a) is the quotient field of F[a]. Hence, it can be characterized,

$$F(a) = \left\{ \frac{f(a)}{g(a)} / \; f, \; g \in F[x], \; g(a) \neq 0 \right\}.$$

$F[x]$, being all polynomials in one indeterminant over F, satisfies the requirements for an integral domain. Let ϕ: $F[x] \rightarrow F[a]$ be defined by,

$$\phi(c_0 + c_1x + \ldots + c_nx^n) = c_0 + c_1a + \ldots + c_na^n.$$

It is an onto ring homomorphism. The kernal of ϕ is an ideal. By the Fundamental Theorem of Ring Homomorphisms we know $\frac{F[x]}{\ker \phi} \simeq F[a]$. So $\frac{F[x]}{\ker \phi}$ is an integral domain and $\ker \phi$ is a prime ideal in $F[x]$. Also $\ker \phi \neq F[x]$ since $\phi(1) \neq 0$. Since F is a field, $F[x]$ is a principal ideal domain, so $\ker \phi = \langle 0 \rangle$ or $\ker \phi = \langle p(x) \rangle$ where $p(x)$ is a non-zero polynomial in $F[x]$. Let us examine these two cases.

Case I: $\ker \phi = \langle 0 \rangle$

Then $F[x] \simeq F[a]$ and the quotient fields $F(x)$ and $F(a)$ are isomorphic. a must be transcendental, since $\ker \phi = \langle 0 \rangle$. Moreover $[F(a):F] = \infty$. Assume $[F(a):F] = n$, n finite, then the $n + 1$ elements $1, a, \ldots, a^n$ are linearly dependent over F. This implies there exist $c_i \in F$, $i = 1, \ldots, n$, such that $c_0 + c_1a + \ldots + c_na^n = 0$ and $c_i \neq 0$ for some i. But then $f(x) = c_0 + c_1x + \ldots + c_nx^n$ is a non-zero polynomial in $F[x]$ where $f(a) = 0$ a contradiction of the assumption that a is transcendental.

Case II: $\ker \phi \neq \langle 0 \rangle$

Since $F[x]$ is a principal ideal domain, $\ker \phi = \langle p(x) \rangle$ for

some $p(x) \in F[x]$. Therefore all polynomials in $F[x]$ that have a as a root are of the form $p(x)f(x)$, where $f(x)$ is an arbitrary polynomial in $F[x]$. $p(x)$ is the lowest degree polynomial in $F[x]$ which has a as a root, since $\deg(p(x)f(x)) = \deg(p(x)) + \deg(f(x)) \geq \deg(p(x))$. We also claim that $p(x)$ is irreducible. If $p(x)$ is reducible, then $p(x) = p_1(x)p_2(x)$. Therefore $p(a) = p_1(a)p_2(a) = 0$, but this implies that either $p_1(a) = 0$ or $p_2(a) = 0$. Then we have a as a root of a polynomial in $F[x]$ that has a smaller degree than $p(x)$, but we have already seen that cannot happen. Since $p(x)$ is irreducible, the ideal $\langle p(x) \rangle$ is maximal and hence $\frac{F[x]}{\langle p(x) \rangle}$ is a field. Now, since $F(a)$ is the smallest subfield of K containing F and a and since $F(a) \supseteq F[a] = \frac{F[x]}{\langle p(x) \rangle}$, we must have $F(a) = F[x]$.

If u is a non-zero element of F, then $\langle p(x) \rangle = \langle up(x) \rangle$. So $p(x)$ is not uniquely determined by the ideal, ker ϕ. But we may normalize $p(x)$ to a monic polynomial.

The $p(x)$ which generates ker ϕ is uniquely determined by:

1) $p(x) \in F[x]$,

2) $p(a) = 0$,

3) $p(x)$ is monic,

4) $p(x)$ is irreducible over F,

5) if $f(x) \in F[x]$ where $f(a) = 0$, then $p(x)$ divides $f(x)$.

To show uniqueness, assume there exists an $f(x) \in F[x]$ satisfying 1) through 4) and that $p(x)$ and $f(x)$ are

relatively prime. Then there exists $g(x)$, $h(x) \in F[x]$ such that $g(x)p(x) + h(x)f(x) = 1$. But the left side of this equation evaluated at a equals zero so $f(x)$ does not exist. From the preceeding discussion we have established the fact that if a is algebraic over F, then $F(a) \simeq F[a]$. Therefore every element of $F(a)$ is of the form $f(a)$ for some $f(x) \in F[x]$.

Def 3.8: The irreducible polynomial $p(x)$ of a over F will be denoted $Irr(a, F)$. The degree of $Irr(a, F)$ is called the degree of a over F and is denoted $deg(a, F)$.

Examples: 1) $p(x) = x^2 - 2$ is monic irreducible over $\mathbb{Q}$, so $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ and $deg(\sqrt{2}, \mathbb{Q}) = 2$.

2) $a = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$ is a zero of

$p(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$,

and by Eisenstien's irreducibility criterion with $p = 2$, $p(x)$ is seen to be irreducible over $\mathbb{Q}$. Therefore $Irr(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$ and $\sqrt{1 + \sqrt{3}}$ is algebraic of degree 4 over $\mathbb{Q}$.

As has been pointed out before, if $F(a)$ is an extension field of F, then $F(a)$ is a vector space over F.

Thm 3.3: Let $F(a)$ be an simple algebraic extension of F with $deg(Irr(a, F)) = n$. Then $\beta = \{1, a, a^2, \ldots, a^{n-1}\}$ is a

basis for F(a) as a vector space over F.

Proof: It must be shown that β spans F(a) and the elements of β are linearly independent.

Let $\gamma \in F(a)$, so $\gamma = f(a)$ for some $f(x) \in F[x]$, where

$$f(x) = b_0 + b_1x + \dots + b_nx^n,\ b_i \in F[x].$$

So $\gamma = b_0 + b_1a + b_2a^2 + \dots + b_na^n$. By the division algorithm there exists $q(x)$, $r(x) \in F[x]$ such that $f(x) = q(x)p(x) + r(x)$, $p(x) = Irr(a, F)$ and $\deg(r(x)) < \deg(p(x)) = n$. Therefore $f(a) = q(a)p(a) + r(a)$ and since $p(a) = 0$, $f(a) = r(a)$. Since r has degree less than n, $f(a) = c_0 + c_1a + \dots + c_ka^k$ where $k \leq n - 1$. Therefore γ is a linear combination of the elements of β.

To show the linear independence of β over F, let

$$b_0 + b_1a + \dots + b_{n-1}a^{n-1} = 0.$$

This implies $f(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$ has a root in F(a). But $\deg(f(x)) \leq n - 1$ so $f(x) \equiv 0$

Corollary 3.4: Let F(a) be a simple algebraic extension of F, then $[F(a):F] = \deg(Irr(a, F)) = n$.

Corollary 3.5: For all $\beta \in F(a)$, β can be written uniquely as $\beta = c_0 + c_1a + \dots + c_{n-1}a^{n-1}$, $c_i \in F$.

Corollary 3.6: Every α of the simple algebraic extension F(a) is algebraic over F.

Proof: Consider the elements $1, \alpha, \dots, \alpha^n$ in F(a), by the

preceeding corollary each of the powers α^k $(0 \leq k \leq n)$ may be written as,

$$\alpha^k = b_{0k} = b_{1k}a + \ldots + b_{n-1\ k}a^{n-1} \quad (k = 0, 1, \ldots, n)$$

Thus we have $n + 1$ equations in the elements $1, a, \ldots, a^{n-1}$ and by eliminating these latter elements it follows that there exists $c_0, c_1, \ldots, c_n \in F$, not all zero for which

$$c_0 \cdot 1 + c_1 \cdot \alpha + \ldots + c_n \cdot \alpha^n = 0.$$

Thus $f(x) = c_0 + c_1 x + \ldots + c_n x^n \in F[x]$ is a non-zero polynomial with $f(\alpha) = 0$. Hence α is algebraic over F.

The next theorem is a summary of the previous results when K is a simple algebraic extension of F and $a \in K$ is algebraic over F.

Thm 3.4: If K:F is a field extension and $a \in K$ is algebraic over F, then:

1) $F(a) \simeq \frac{F[x]}{\langle p(x) \rangle}$, where $p(x) \in F[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $p(a) = 0$ and $g(a) = 0$, for $g(x) \in F[x]$ iff $p(x) | g(x)$.

2) $F(a) \simeq F[a]$

3) $\{1, a, a^2, \ldots, a^{n-1}\}$ is a basis for F(a) as a vector space over F

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

5) Every element of F(a) can be written uniquely in the form $c_0 \cdot 1 + c_1 a + \ldots + c_{n-1} a^{n-1}$, with $c_i \in F$.

Example: Let $K = \mathbb{R}$ and $F = \mathbb{Q}$ and $p(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$. $p(x)$ is irreducible and monic over $\mathbb{Q}$. It has at least one real root $a \in \mathbb{R}$. Let $\beta \in \mathbb{Q}(a)$ and look at how β can be written as $\beta = c_0 + c_1 a + c_2 a^2$.

Take $\beta = a^4 + 2a^3 + 3$, so

$f(x) = x^4 + 2x^3 + 3$

$= (x^3 - 3x - 1)(x + 2) + (3x^2 + 7x + 5)$, so

$a^4 + 2a^3 + 3 = (a^3 - 3x - 1)(a + 2) + (3a^2 + 7x + 5)$.

Therefore $\beta = 3a^2 + 7x + 5$.

The multiplicative inverse of $3a^2 + 7a + 5$ in $\mathbb{Q}(a)$ may be calculated as follows; since $x^3 - 3x - 1$ is irreducible in $\mathbb{Q}[x]$, the polynomials $p(x) = x^3 - 3x - 1$ and $f(x) = 3x^2 + 7x + 5$ are relatively prime in $\mathbb{Q}[x]$. Hence there exists polynomials $g(x)$, $h(x) \in \mathbb{Q}[x]$ such that

$(x^3 - 3x - 1)g(x) + (3x^2 + 7x + 5)h(x) = 1 \Rightarrow$

$(a^3 - 3a - 1)g(a) + (3a^2 + 7a + 5)h(a) = 1 \Rightarrow$

$(3a^2 + 7a + 5)h(a) = 1$.

Therefore, $h(a) \in \mathbb{Q}[a]$ is the inverse of $3a^2 + 7a + 5$. One can compute $h(a) = \frac{7}{111}a^2 - \frac{26}{111}a + \frac{28}{111}$ by the Euclidean Algorithm.

If two fields are isomorphic, what conditions on extensions of these fields will make the extensions isomorphic.

Thm 3.5: Let ϕ: $E \to F$ be a field isomorphism and α is an

element of some extension field of E and β is an element of some extension field of F. Assume that either:

1) α and β are both transcendental over E and F respectively, or

2) α is the root of an irreducible polynomial $f(x) \in E[x]$ and β is the root of $\bar{\phi}(f(x)) \in F[x]$, where $\bar{\phi}: E[x] \to F[x]$ is the extension of $\phi: E \to F$.

Then ϕ extends to an isomorphism $\hat{\phi}: E(\alpha) \to F(\beta)$, where $\hat{\phi}(\alpha) = \beta$.

Proof: 1) Let $\phi: E \to F$ be a field isomorphism. It has an extension to a ring isomorphism $\bar{\phi}: E[x] \to F[x]$ defined by:

$$\bar{\phi}(f(x)) = \bar{\phi}(c_0 + c_1x + \dots + c_nx^n) \quad c_i \in E$$
$$= (\phi(c_0) + \phi(c_1)x + \dots + \phi(c_n)x^n) \in F[x].$$

First we will show $\bar{\phi}$ is an isomorphism. Assume $m < k$

$$\bar{\phi}((c_0 + c_1x + \dots + c_nx^n) + (b_0 + b_1x + \dots + b_kx^k))$$
$$= \bar{\phi}((c_0 + b_0) + (c_1 + b_1)x + \dots + (c_n + b_n)x^n + \dots + b_kx^k)$$
$$= \phi(c_0 + b_0) + \phi(c_1 + b_1)x + \dots + \phi(c_n + b_n)x^n + \dots + \phi(b_k)x^k$$
$$= \phi(c_0) + \phi(b_0) + \dots + \phi(c_n)x^n + \phi(b_n)x^n + \dots + \phi(b_k)x^k$$
$$= \phi(c_0) + \phi(c_1)x + \dots + \phi(c_n)x^n + \phi(b_0) + \phi(b_1)x + \dots + \phi(b_k)x^k$$
$$= \bar{\phi}(c_0 + c_1x + \dots + c_nx^n) + \bar{\phi}(b_0 + b_1x + \dots + b_kx^k), \text{ and}$$

addition is preserved.

Consider $\bar{\phi}((c_0 + c_1x + \dots + c_nx^n)(b_0 + b_1x + \dots + b_kx^k))$. Multiplying inside the parenthesis, the terms of the product will have the form $(\sum c_ib_j)x^r$, where $i + j = r$ and $r \leq m + k$. Then $\bar{\phi}$ acts on this product by $\phi(\sum c_ib_j)x^r$ and

hence $\left(\sum\phi(c_i)\phi(b_j)\right)x^r$. But this will factor to

$\left(\phi(c_0) + \phi(c_1)x + \ldots + \phi(c_s)x^s\right)\left(\phi(b_0) + \phi(b_1)x + \ldots + \phi(b_k)x^k\right) =$

$\bar{\phi}(c_0 + c_1x + \ldots + c_sx^s)\bar{\phi}(b_0 + b_1x + \ldots + b_kx^k)$, and multiplication is preserved. Assuming $\bar{\phi}$ is not 1-1 or onto will force ϕ to also not be 1-1 or onto.

$\bar{\phi}$ can be extended to ψ: $E(x) \to F(x)$ on the quotient fields of E[x] and F[x] by $\psi\left(\frac{f(x)}{g(x)}\right) = \frac{\bar{\phi}\left(f(x)\right)}{\bar{\phi}\left(g(x)\right)}$. We will now show that ψ is an isomorphism.

Let $m(x)$, $n(x) \in E(x)$, so $m(x) = \frac{f(x)}{g(x)}$ and $n(x) = \frac{h(x)}{j(x)}$, for some $f(x)$, $g(x)$, $h(x)$, $j(x) \in E[x]$, where $g(x)$, $j(x) \neq 0$.

$$\psi\left(m(x) + n(x)\right) = \psi\left(\frac{f(x)}{g(x)} + \frac{h(x)}{j(x)}\right) = \psi\left(\frac{f(x)j(x) + g(x)h(x)}{g(x)j(x)}\right) =$$

$$\frac{\bar{\phi}\left(f(x)j(x) + g(x)h(x)\right)}{\bar{\phi}\left(g(x)j(x)\right)} = \frac{\bar{\phi}\left(f(x)\right)\bar{\phi}\left(j(x)\right) + \bar{\phi}\left(g(x)\right)\bar{\phi}\left(h(x)\right)}{\bar{\phi}\left(g(x)\right)\bar{\phi}\left(j(x)\right)} =$$

$$\frac{\bar{\phi}\left(f(x)\right)}{\bar{\phi}\left(g(x)\right)} + \frac{\bar{\phi}\left(h(x)\right)}{\bar{\phi}\left(j(x)\right)} = \psi\left(\frac{f(x)}{g(x)}\right) + \psi\left(\frac{h(x)}{j(x)}\right) = \psi\left(m(x)\right) + \psi\left(n(x)\right)$$

and addition is preserved. For multiplication, let $m(x)$ and $n(x)$ be as described for addition, then

$$\psi\left(\frac{f(x)}{g(x)}\cdot\frac{h(x)}{j(x)}\right) = \psi\left(\frac{f(x)h(x)}{g(x)j(x)}\right) = \frac{\bar{\phi}\left(f(x)h(x)\right)}{\bar{\phi}\left(g(x)j(x)\right)} = \frac{\bar{\phi}\left(f(x)\right)\bar{\phi}\left(h(x)\right)}{\bar{\phi}\left(g(x)\right)\bar{\phi}\left(j(x)\right)} =$$

$$\frac{\bar{\phi}\left(f(x)\right)}{\bar{\phi}\left(g(x)\right)}\cdot\frac{\bar{\phi}\left(h(x)\right)}{\bar{\phi}\left(j(x)\right)} = \psi\left(\frac{f(x)}{g(x)}\right)\psi\left(\frac{h(x)}{j(x)}\right)$$

and multiplication is preserved.

Now we have, $E(\alpha) \simeq E(x) \simeq F(x) \simeq F(\beta)$, so $E(\alpha) \simeq F(\beta)$.

2) Let $f(x) \in E[x]$ where $f(\alpha) = 0$ and $f(x)$ is monic irreducible.

To show $\bar{\phi}\left(f(x)\right)$ is irreducible over F[x], we assume it is not. Then there exists $f_1(x)$, $f_2(x) \in F[x]$ such that

$\bar{\phi}(f(x)) = f_1(x)f_2(x)$. Since $\bar{\phi}$ is an isomorphism, there exists $\bar{\phi}^{-1}(f_1(x))$, $\bar{\phi}^{-1}(f_2(x)) \in E[x]$ and

$f(x) = \bar{\phi}^{-1}(f_1(x))\bar{\phi}^{-1}(f_2(x))$ and is reducible.

The maps π: $\frac{E[x]}{<f(x)>} \rightarrow E[\alpha] \simeq E(\alpha)$ and

ψ: $\frac{F[x]}{<\bar{\phi}(f(x))>} \rightarrow F[\beta] \simeq F(\beta)$,

where $\pi(g(x) + <f(x)>) = g(\alpha)$ and $\psi(h(x) + <\bar{\phi}(f(x))>) = h(\beta)$ are isomorphisms.

The map θ: $\frac{E[x]}{<f(x)>} \rightarrow \frac{F[x]}{<\bar{\phi}(f(x))>}$ given by

$\theta(g(x) + <f(x)>) = \bar{\phi}(g(x)) + <\bar{\phi}(f(x))>$ is an isomorphism.

Therefore the composition

$E(\alpha) \overset{\pi^{-1}}{\rightarrow} \frac{E[x]}{<f(x)>} \overset{\theta}{\rightarrow} \frac{F[x]}{<\bar{\phi}(f(x))>} \overset{\psi}{\rightarrow} F(\beta)$ is an isomorphism of fields such that $(\psi \circ \theta \circ \pi^{-1})(\alpha) = \beta$.

A corollary of this theorem is that an isomorphism of a field extension exists which sends roots of an irreducible polynomial to each other, but leaves the base field unchanged.

Corollary 3.7: Let K and L be extension fields of F and let $\alpha \in K$ and $\beta \in L$ be algebraic over F. Then α and β are roots of the same irreducible polynomial $f(x) \in F[x]$ iff there is an isomorphism of fields $F(\alpha) \simeq F(\beta)$ which sends α onto β and is the identity on F. (In particular if K = L!)

Proof: For the "if" part of this theorem we can apply the previous theorem with ϕ being the identity on F, so that $\bar{\phi}(f) = f$, for all $f \in F[x]$.

For the "only if" part, suppose $\eta: F[\alpha] \xrightarrow{\cong} F[\beta]$ with $\eta(\alpha) = \beta$ and $\eta(\mu) = \mu$ for all $\mu \in F$. Let $f(x) \in F[x]$ be the irreducible polynomial of the algebraic element α. If $f(x) = \sum_{i=0}^{n} u_i x^i$, where $u_i \in F$, then $0 = f(a) = \sum_{i=0}^{n} u_i a^i$. therefore

$$0 = \eta\left(\sum_{i=0}^{n} u_i a^i\right) = \sum_{i=0}^{n} \eta\left(u_i a^i\right) = \sum_{i=0}^{n} \eta(u_i)\eta(a^i) = \sum_{i=0}^{n} u_i\left(\eta(a)\right)^i = \sum_{i=0}^{n} u_i b^i = f(\beta).$$

The point of the previous theorem is that given an isomorphism $\phi: E \to F$ between fields, it can be extended to an isomorphism between the larger fields $E(\alpha)$ and $F(\beta)$ Such extension theorems, saying that, under suitable conditions, maps between "sub-objects" can be extended to maps between "objects", constitute an important technique in mathematics. Since, with the given hypotheses, the extensions $E(\alpha):E$ and $F(\beta):F$ are isomorphic, we can identify E with F and $E(\alpha)$ with $F(\beta)$ via the isomorphism between them.

So far we assumed we are given an extension field K of F and adjunction of elements to F took place in K. Our next two theorems show it is really not necessary to have K given in advance.

Thm 3.6: If F is a field, then there exists a simple transcendental extension of F.

Proof: Let F(x) be the field of all rational funtions of

an indeterminate x with coefficients in F, i.e. F(x) is the field of quotients of the integral domain F[x]. So F(x) is a simple transcendental extension of F. The uniqueness of F(x) up to isomorphism follows from the previous theorem.

Now we want to look at algebraic extensions of a field. As we have seen previously, if we have a simple algebraic extension F(a), there exists an irreducible polynomial $p(x) \in F[x]$ such that $p(a) = 0$. We will now start with an irreducible polynomial in F[x] and then construct an extension field of F in which the polynomial has a root.

Thm 3.7 (Kronecker): Let F be a field and p(x) be an irreducible polynomial over F. Then there exists a simple extension, E of F, such that p(x) has a zero in E.

Proof: Since $p(x) = a_0 + a_1x + \dots + a_nx^n$ is irreducible in F, $\langle p(x) \rangle$ is maximal ideal in F[x], so $\frac{F[x]}{\langle p(x) \rangle}$ is a field. Let $E = \frac{F[x]}{\langle p(x) \rangle}$. Define $\psi: F \to \frac{F[x]}{\langle p(x) \rangle}$ by $\psi(a) = a + \langle p(x) \rangle$. Let $\psi(a) = \psi(b)$, so $a + \langle p(x) \rangle = b + \langle p(x) \rangle$, which implies $a - b \in \langle p(x) \rangle$, which in turn implies that $a - b = p(x)q(x)$ for some $q(x) \in F[x]$ with $\deg(q(x)) \leq n$. But $a - b \in F$, so $a - b = 0$ and $a = b$. Thus ψ is one-to-one.

$$\psi(a + b) = (a + b) + \langle p(x) \rangle$$

$$= \left(a + \langle p(x) \rangle\right) + \left(b + \langle p(x) \rangle\right) = \psi(a) + \psi(b), \text{ also}$$

$$\psi(ab) = ab + \langle p(x) \rangle = \left(a + \langle p(x) \rangle\right)\left(b + \langle p(x) \rangle\right)$$

$$= \psi(a)\psi(b),$$

so ψ is a homomorphism.

Let $\alpha = x + \langle p(x) \rangle \in \frac{F[x]}{\langle p(x) \rangle}$

$$p(\alpha) = a_0 + a_1\left(x + \langle p(x) \rangle\right) + \ldots + a_n\left(x + \langle p(x) \rangle\right)^n =$$

$$(a_0 + a_1 x + \ldots + a_n x^n) + \langle p(x) \rangle = p(x) + \langle p(x) \rangle =$$

$$\langle p(x) \rangle = 0$$

Example: Let $F = \mathbb{R}$, and let $f(x) = x^2 + 1$. This is irreducible in $\mathbb{R}$, so $\langle (x^2 + 1) \rangle$ is maximal in $\mathbb{R}[x]$ and $\frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle}$ is a field. Each $r \in \mathbb{R}$ is identified with

$$r + \langle x^2 + 1 \rangle \in \frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle},$$

so $\mathbb{R}$ can be viewed as a subfield of $\frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle}$. If we let $\alpha = x + \langle x^2 + 1 \rangle$, then

$$\alpha^2 + 1 = (x + \langle x^2 + 1 \rangle)^2 + (1 + \langle x^2 + 1 \rangle) =$$

$$(x^2 + 1) + \langle x^2 + 1 \rangle = 0, \text{ and } \alpha \text{ is a zero of } x^2 + 1.$$

$\frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle}$ is isomorphic to the field of complex numbers.

Splitting Fields

If $f(x) \in F[x]$ is an irreducible polynomial over F, we know there exists a field $F(a)$, where $f(a) = 0$. $f(x)$ will factor in this field to $f(x) = (x - a)g(x)$, where $g(x)$ may or may not be reducible over $F(a)$. If it is irreducible over $F(a)$ we can continue and find a field in which $g(x)$ will factor. We want to find the smallest field where $f(x)$ will factor completely.

Def 3.9: Let $f(x) \in F[x]$, where $\deg(f(x)) \geq 1$. An extension field E:F is a splitting field for $f(x)$ over F iff:

1) $f(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$ $r_i \in E$, $c \in F$

2) $E = F(r_1, r_2, \ldots, r_n)$, i.e. E is generated by the roots $r_1, \ldots, r_n$ of $f(x)$ in E.

Examples: 1) $\mathbb{Q}(\sqrt{2})$ is a splitting field for $f(x) = x^2 - 2$ in $\mathbb{Q}[x]$ since $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

2) $\mathbb{C}$ is the splitting field for $f(x) = x^2 + 1$ over $\mathbb{R}$.

As usual, it is nice to know something exists before we spend much time talking about it.

Thm 3.8: If F is a field and $f(x) \in F[x]$ is of positive degree n, there exists a splitting field E for $f(x)$ over F.

Proof: Let $f(x) = c\, f_1(x)\, f_2(x) \cdots f_k(x)$ be the factorization of $f(x)$ into monic irreducible factors. $k \leq n = \deg(f(x))$. If $n - k = 0$ then all the factors $f_i(x)$ are linear, and F is the splitting field of $f(x)$. Assume $n - k > 0$, so that one of the factors, $f_i(x)$, is of degree less than one. We can further assume that it is $f_1(x)$. Let $K = \frac{F[x]}{\langle f_1(x) \rangle}$. Since f_1 is irreducible, K is an extension field of F and $K = F(r_1)$, where $r_1 = x + \langle f_1(x) \rangle$ is a root of $f_1(x) = 0$. Since $F \subset F(r_1) = K$ and $f(x)$ and the factors $f_i(x) \in F[x] \subset K[x]$, we obtain the following factorization

of f(x) into monic irreducible polynomials in K[x].

$$f(x) = c(x - r_1)\, g_1(x)\, g_2(x) \cdots g_i(x),$$

where $g_1, \ldots, g_i$ are irreducible over $K = F(r_1)$. If all the g_i's are of degree 1, then $F(r_1)$ contains all the roots of $f(x) = 0$. Otherwise, let $g_1(x)$ be of degree > 1. By adjoining a root r_2 of $g_1(x)$ to $F(r_1)$ we obtain the field $F(r_1, r_2)$ and f(x) will factor in $F(r_1, r_2)[x]$ to the following form,

$$f(x) = c\,(x - r_1)\,(x - r_2)\, h_1(x) \cdots h_t(x).$$

If not all the irreducible factors $h_i(x)$ are of degree 1, we can continue in the same manner. Each adjunction of a root of an irreducible factor of f(x) will add at least one new linear factor of f(x). Hence after a finite number of adjunctions we obtain a field $F(r_1, \ldots, r_s)$, such that in $F(r_1, \ldots, r_s)[x]$ the polynomial f(x) splits into linear factors,

$$f(x) = c\,(x - r_1) \ldots (x - r_n).$$

In other words $F(r_1, \ldots, r_s)$ contains all the roots of f(x), i.e.

$$F(r_1, \ldots, r_s) = F(r_1, \ldots, r_s, r_{s+1}, \ldots, r_n).$$

Clearly the number of adjunctions which is necessary to arrive at $F(r_1, \ldots, r_n)$ does not exceed $n - 1$.

After we establish existence, the next question to look at is uniqueness. To do so we first look at the following.

Lemma 3.2: Let σ: $F \to F'$ be a field isomorphism. Let $p(x) \in F[x]$ and $\sigma(p(x)) \in F'[x]$. Let E be a splitting field for $p(x)$ over F and E' a splitting field for $\sigma(p(x))$. Then σ can be extended to an isomorphism $\bar{\sigma}$: $E \to E'$, such that $\bar{\sigma}|_F = \sigma$.

Proof: The proof is by induction on the number k of roots of $p(x)$ outside F. Let $p(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$ be the factored form of $p(x)$ in E. If all the roots of $p(x)$ are in F, i.e. $k = 0$, then $E = F$. Since isomorphisms preserve operations $\sigma(p(x)) = \sigma(c)(x - \sigma(r_1)) \cdots (x - \sigma(r_n))$ is the factored form of $\sigma(p(x))$ in E'. This is a polynomial in F' and $E' = F'$. So σ is itself the required extension.

To proceed by induction, we will make the following assumption. Let K and K' be fields such that $F \subset K \subseteq E$ and $F' \subset K' \subseteq E'$, and let σ_1 be an extension of σ to an isomorphism of K onto K'. If fewer than k roots of $p(x)$ are outside K, then there exists an extension of σ_1 to an isomorphism $\bar{\sigma}$ of E onto E'.

Factor $p(x)$ into $f_1(x)f_2(x) \cdots f_n(x)$, all irreducible in F. Not all these factors can be of degree 1, since then $p(x)$ would split in F. Let $\deg(f_1(x)) = r > 1$, where $r < k$. $\sigma(p(x))$ will factor to $\sigma(f_1(x)) \cdots \sigma(f_n(x))$ in F'. $\sigma(f_1(x))$ must be irreducible in F'. If it were not, σ^{-1} would induce a factorization of $f_1(x)$ in F. $\deg(\sigma(f_1(x)))$ must also be greater than 1. Let α_1 and α'_1 be roots of $f_1(x)$ and $\sigma(f_1(x))$. Let $K = F(\alpha)$ and $K' = F'(\alpha'_1)$. By Thm 3.5, σ can

be extended to an isomorphism σ_1: K → K'. We now regard p(x) and $\sigma(p(x))$ as polynomials in K[x] and K'[x]. The number of roots of p(x) outside K is less than k, thus by our induction hypothesis we can extend σ_1 and hence σ to an isomorphism $\bar{\sigma}$: E → E'.

By taking the identity isomorphism i: F → F, we have the following theorem.

Thm 3.9: If E is the splitting field of f(x) over F, then E is unique up to isomorphism.

Proof: Let E' be any other splitting field of f(x) over F and let i: F → F be the identity automorphism of F. The above lemma implies there exists an extension of i to an isomorphism $\bar{i}$: E → E'.

Examples: 1) Let $f(x) = (x^2 - 3)(x^3 + 1) \in \mathbb{Q}[x]$.

$$f(x) = \left(x + \sqrt{3}\right)\left(x - \sqrt{3}\right)(x + 1)\left(x - \frac{-1 + i\sqrt{3}}{2}\right)\left(x - \frac{-1 - i\sqrt{3}}{2}\right)$$

The splitting field of f(x) is $\mathbb{Q}\left(\sqrt{3}, \frac{-1 + i\sqrt{3}}{2}\right) = \mathbb{Q}\left(\sqrt{3}, i\right)$

2) $f(x) = \left(x^2 - 2x - 2\right)\left(x^2 + 1\right)$. The splitting field of f(x) is again $\mathbb{Q}\left(\sqrt{3}, i\right)$

3) Let $f(x) = x^2 + x + 1$ and $F = \mathbb{Z}_2 = (0, 1)$

$f(0) = 1$ and $f(1) = 1 + 1 + 1 = 1$

$$K = \frac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1\rangle}$$

$r = x + \langle x^2 + x + 1\rangle$ is a zero of f(x)

The elements of the splitting field are:

$\bar{0} = 0 + \langle x^2 + x + 1 \rangle$ This is the Galois Field

$\bar{1} = 1 + \langle x^2 + x + 1 \rangle$ $GF(2^2)$

$r = x + \langle x^2 + x + 1 \rangle$

$r + 1 = (1 + x) + \langle x^2 + x + 1 \rangle$

f will factor as $f(x) = (x + r)(x - r)$

Algebraic Extensions

In studying the zeros of polynomials in F[x], we shall be interested in extension fields of F which contain only elements that are algebraic over F.

Def 3.10: E:F is an algebraic extension iff every $a \in E$ is algebraic over F.

Again we examine the question of existence with the following theorem.

Thm 3.10: Every finite extension is algebraic.

Proof Let E:F be finite, i.e., [E:F] = n and let $a \in E$ The n + 1 elements $\{1, a, a^2, \ldots, a^n\}$ are linearly dependent over E. So there exists $c_0, c_1, \ldots, c_n \in F$ such that

$c_0 + c_1a + \ldots + c_na^n = 0$ and at least one $c_i \neq 0$. So let $f(x) = c_0 + c_1x + \ldots + c_nx^n \in F[x]$ and $f(a) = 0$. So a is algebraic over F.

The converse of this is not true, there exists algebraic extensions that are not finite. We will examine a few facts about algebraic extensions, and then look at an example of an infinite algebraic extension.

As a corollary to Thm 3.10 we have:

Corollary 3.8: Every finite extension of F can be obtained by the adjunction of finitely many algebraic elements to F. Conversely, every extension field obtained by the adjunction of finitely many algebraic elements to F is of finite degree and hence algebraic.

So if $[E:F] < \infty$, then $E = F(a_1, a_2, \ldots, a_n)$, where each a_i is algebraic over F.

Corollary 3.9: Let E:F be any extension. If a, b $\in$ E are algebraic over F, then a $\pm$ b and a/b (b $\neq$ 0) are algebraic over F.

Proof: F(a, b) is an algebraic extension of F and a $\pm$ b, a/b $\in$ F(a, b) and F(a, b) $\subseteq$ E.

This is equivalent to saying the set of all algebraic elements in E:F is a subfield of E.

Example. Let A be the set of all algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$. A:$\mathbb{Q}$ is algebraic and we claim $[A:\mathbb{Q}] = \infty$. Consider the sequence of primes 2, 3, 5, 7, ... , p_n, ... If we consider the sequence of extensions $K_n = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p_n})$, then $[K_n:\mathbb{Q}] = 2^n$ and $[A:\mathbb{Q}] \geq [K_n:\mathbb{Q}]$ for all n. A is an algebraic extension of infinite degree.

Thm 3.11: Let L:E be algebraic and E:F be algebraic, then L:F is algebraic.

Proof: We need to show $[L:F] < \infty$, so let $\alpha \in L$. Let $p(x) = c_0 + c_1x + \ldots + c_nx^n$ be the minimal polynomial of α over F. α is algebraic over $F(c_0, c_1, \ldots, c_n)$.

$$[F(c_0, c_1, \ldots, c_n)(\alpha) : F(c_0, c_1, \ldots, c_n)] =$$

$$[F(c_0, c_1, \ldots, c_n, \alpha) : F(c_0, c_1, \ldots, c_n)] < \infty$$

Also $[F(c_0, c_1, \ldots, c_n) : F] < \infty$.

$$[F(\alpha):F] \leq [F(c_0, \ldots, c_n, \alpha) : F] =$$

$$[F(c_0, \ldots, c_n, \alpha) : F(c_0, \ldots, c_n)][F(c_0, \ldots, c_n) : F] < \infty$$

So α is algebraic over F and L:F is algebraic.

Normal Extensions

In this section and the next we will examine two important properties of an extension. The first ensures good behavior for splitting polynomials and for the extendibility of monomorphisms.

Def 3.11: Let E:F. E is a normal extension of F iff E is algebraic over F and if $f(x) \in F[x]$ is irreducible, then either f(x) splits in E or f(x) has no roots in E.

This is equivalent to saying: E is normal over F iff E is algebraic over F and every irreducible polynomial $f(x) \in F[x]$ that has a root in E, splits in E. A third equivalent definition is: E is normal over F iff E is algebraic over F and the minimal irreducible polynomial over F of every element in E splits in E.

Examples:

1) $\mathbb{C}$ is a normal extension of $\mathbb{R}$.

2) $\mathbb{R}$ is not a normal extension of $\mathbb{Q}$. To see this consider $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. f(x) is irreducible over $\mathbb{Q}$ and has one root in $\mathbb{R}$, namely $\sqrt[3]{2}$. But it does not split in $\mathbb{R}$ since the other two roots are complex.

3) If E:F and [E:F] = 2, then E is a normal extension of F. Let $a \in E$, $a \notin F$. Let p(x) be the minimal irreducible polynomial of a over F. Then $[F(a):F] = \deg(p(x)) > 1$. $[E:F] = [E:F(a)][F(a):F] = 2$, so $[E:F(a)] = 1$ and $[F(a):F] = 2$. So $E = F(a)$ and $\deg(p(x)) = 2$. Since one root of p(x) is in E, the other root must also be in E. So p(x) splits is E and E is normal over F.

Not all finite extensions are normal extensions, for example $\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}$ is not normal over $\mathbb{Q}$. The next theorem gives a necessary and sufficient condition for a finite extension to be normal.

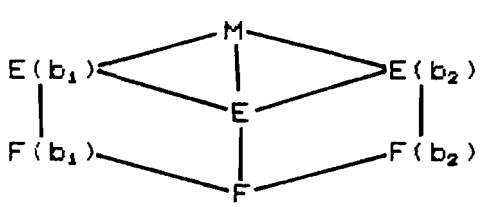
Thm 3.12: Let E be an extension of a field F. The following are equivalent.

1) E is a finite normal extension of F.

2) E is the splitting field over F of some $f(x) \in F[x]$.

Proof: Let E be a finite normal extension of F. Then $E = F(a_1, \ldots, a_n)$ where $a_i \in E$. Each a_i is algebraic over F. Let f_i be the minimal polynomial of a_i over F and let $f = f_1 \cdot f_2 \cdot \cdots \cdot f_n$. By construction each f_i splits in E. Since E is generated by F and the zero's of f, it is the splitting field for f.

Suppose E is the splitting field over F for some $f(x) \in F[x]$. Then $[E:F] < \infty$, so E is algebraic over F. Let g be an irreducible polynomial over F with a zero in E. Let M be the splitting field for $f(x) \cdot g(x)$. Since E is the splitting field of f(x) over F, we may assume $E \subseteq M$. Let b_1, b_2 be two zeros of g in M. Consider the following tower of fields:



For $i = 1$ or 2

$[E(b_i):E][E:F] = [E(b_i):F] = [E(b_i):F(b_i)][F(b_i):F]$. Also

$[F(b_1):F] = \deg(f(x)) = [F(b_2):F]$

There exists an isomorphism, ϕ: $F(b_1) \to F(b_2)$, such that $\phi|_F = Id_F$. $E(b_1)$ is the splitting field for $f(x)$ over $F(b_1)$ and $E(b_2)$ is the splitting field for $\phi(f(x))$ over $E(b_2)$ So ϕ extends to an isomorphism $\bar{\phi}$: $E(b_1) \to E(b_2)$. So we have

$[E(b_1):F(b_1)] = [E(b_2):F(b_2)]$

Simple arithmetic gives $[E(b_1):E] = [E(b_2):E]$. If b_1 is in E, $[E(b_1):E] = 1$. This will force b_2 to be in E, since $[E(b_2):E] = 1$ and therefore E is normal over F.

Thm 3.13: Let K be a field Let L be an extension of K and M an extension of L. So $M:L:K$. If $M:K$ is normal, then $M:L$ is normal

Proof: Since $[M:K] = [M:L][M:K] < \infty$, $M:L$ is algebraic Let $a \in M$ The minimal polynomial of a over L is a factor in $L[x]$ of the minimal polynomial of a over K. Since the latter splits in M so does the former.

Monomorphisms, Automorphisms, and Normal Closures

In the last theorem we have seen if $M:K$ is a normal extension then M is normal over any intermediate field L. However, L is not automatically normal over K, as seen in the next example.

Example: Let ω be the complex cube root of 1, so $\omega = \frac{-1 + i\sqrt{3}}{2}$ $\mathbb{Q}(\sqrt[3]{2}, \omega):\mathbb{Q}$ is normal since $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field for $f(x) = x^3 - 2$, but $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ is not normal since $f(x) = x^3 - 2$ does not split in $\mathbb{Q}(\sqrt[3]{2})$.

We will now look at conditions that will force L:K to be normal.

Def 3.12: Suppose K is a subfield of the fields M and L. A K-monomorphism of M into L is a field monomorphism ϕ: M $\rightarrow$ L such that $\phi(k) = k$ for all $k \in K$.

If the mapping ϕ in the preceeding definition happens to be an automorphism, then ϕ will be called a K-automorphism. If $K \subseteq M \subseteq L$, then any K-automorphism of L can be restricted to a K-monomorphism of M into L. We will look at when this process can be reversed.

Thm 3.14: Let L:K be a finite normal extension and M an intermediate field. Let ϕ: M $\rightarrow$ L be a K-monomorphism. Then there exists a K-automorphism σ: L $\rightarrow$ L such that $\sigma|_M = \phi$.

Proof: Let L:K be a finite normal extension. So L is a splitting field over K of some polynomial f(x) over K. Since $K \subseteq M$, L is a splitting field of f(x) over M and also

a splitting field for $\phi(f(x))$ over $\phi(M)$, but $\phi|_K = Id_K$, so $\phi(f(x)) = f(x)$. Consider the diagram:

$$\begin{array}{ccc} M & \rightarrow & L \\ \phi\downarrow & & \downarrow\sigma \\ \phi(M) & \rightarrow & L \end{array}$$

By the uniqueness of splitting fields, there exists an isomorphism $\sigma: L \rightarrow L$, such that $\sigma|_M = \phi$. Therefore σ is an automorphism of L. Since $\sigma|_K = \phi|_K = Id_K$, σ is a K-automorphism.

This allows us to construct K-automorphisms as follows.

Thm 3.15: Let L:K be a finite normal extension and α, β are zeros in L of the irreducible polynomial p(x) over K. Then there exists a K-automorphism $\sigma: L \rightarrow L$ such that $\sigma(\alpha) = \beta$.

Proof: Since α and β are zeros of the same irreducible polynomial $p(x) \in K[x]$, there is an isomorphism $\phi: K(\alpha) \rightarrow K(\beta)$ such that $\phi|_K = Id_K$ and $\phi(\alpha) = \beta$. By the previous theorem, ϕ extends to a K-automorphism $\sigma: L \rightarrow L$.

If an extension is not normal, we would like to recover normality by making the extension larger. If it is not normal, then it does not contain all roots of a polynomial. So perhaps by adding elements to the extension we can gain all the roots. As is usually the case, we would like to add as little as possible to obtain a normal extension.

Def 3.13: Let L be an algebraic extension of K. A normal closure of L:K is an extension N:L such that:

1) N:K is normal

2) If $L \subseteq M \subseteq N$ and M:K is normal then $N = M$.

That is, N is the smallest extension that is normal over K.

This definition implies that if L:K is a normal extension, then the normal closure of L:K is L. We will begin by looking at the existence and uniqueness of the normal closure with the following theorem.

Thm 3.16: If L:K is a finite extension, then there exists a normal closure N which is a finite extension of K. If M is another normal closure of L:K, then M:K and N:K are isomorphic.

Proof: Let $\{a_1, a_2, \ldots, a_r\}$ be a basis for L over K and let $m_i(x)$ be the minimal polynomial for a_i over K. Let N be the splitting field for $f(x) = m_1(x) \cdot m_2(x) \cdot \cdots \cdot m_r(x)$ over L, then N is the splitting field for f(x) over K and N:K is normal and finite. Let P:K such that $L \subseteq P \subseteq N$ and P:K is normal Each polynomial $m_i(x)$ has a zero a_i in P, and so splits in P. Since N is the splitting field, $P = N$, and N is the normal closure.

Let M and N be normal closures of L:K. f(x) splits in both M and N, so M and N each contain a splitting field for f(x). These splitting fields contain L and are normal over

K, so they must be equal M and N respectively. By uniqueness of splitting fields M:K and N:K are isomorphic.

Lemma 3.3: Let $K \subseteq L \subseteq N \subseteq M$ be fields where L:K is finite and N is the normal closure of L:K. Let ϕ: $L \to M$ be a K-monomorphism. Then $\phi(L) \subseteq N$.

Proof: Let $\alpha \in L$ and let $m(x)$ be the minimal polynomial of α over K. Then

$$0 = m(\alpha) = \phi\big(m(\alpha)\big) = m\big(\phi(\alpha)\big),$$

so $\phi(\alpha)$ is a zero of $m(x)$ and must lie in N since N:K is normal. Therefore $\phi(L) \subseteq N$.

This result allows us to concentrate on the normal closure when looking at monomorphisms of extensions. We get sort of a converse of this with the next theorem.

Thm 3.17: For a finite extension L:K, the following are equivalent:

1) L:K is normal

2) There exists a normal extension N of K containing L such that every K-monomorphism ϕ: $L \to N$ is a K-automorphism of L.

3) For every normal extension M of K containing L, every K-monomorphism ϕ: $L \to M$ is a K-automorphism.

Proof: 1) $\Rightarrow$ 3) Let L:K be a normal extension, then L is the normal closure of L:K. So for a K-monomorphism

ϕ: L $\rightarrow$ L, ϕ(L) $\subseteq$ L. But ϕ is a K-linear map on the finite dimensional vector space L over K. So ϕ(L) has the same dimension as L, therefore ϕ(L) = L and ϕ is a K-automorphism.

3) $\Rightarrow$ 2) The existence of the normal closure N is given by a previous theorem.

2) $\Rightarrow$ 1) Let f be an irreducible polynomial over K with a zero $\alpha \in$ L. Then f splits over N since N:K is normal. If β is a zero of f in N, there exists an automorphism σ: N $\rightarrow$ N, such that $\sigma(\alpha) = \beta$. By hypothesis σ is a K-automorphism of L so $\beta = \sigma(\alpha) \in \sigma(L) = L$. Therefore f splits in L and L is normal over K.

Separable Extensions

We now look at a property of extensions called separability. Galois did not mention the concept of separability explicitly since he worked only in the field of complex numbers, in which separability is automatic. In fact any field of charateristic zero is automatically separable. Problems arise is fields of non-zero characteristic. Separability deals with the lack of multiple roots of irreducible polynomials over the field.

Def 3.14: Let K be a splitting field of a polynomial f(x) $\in$ F[x]. Let α be a root of f(x). α is said to be of

multiplicity r iff r is the greatest integer such that $(x - \alpha)^r$ divides f(x) in K[x]. If $r = 1$, then α is a simple root of f(x), and if $r > 1$, then α is a multiple root.

Thm 3.18: Let $f(x) \in F[x]$ be irreducible over F. Then all roots of f(x) in a splitting field K of f(x) have the same multiplicity.

Proof Let α and β be two roots of f(x) in K. There exists an isomorphism $\phi: F(\alpha) \to F(\beta)$, where $\phi(\alpha) = \beta$, which will extend to $\bar{\phi}: K \to K$. If α has multiplicity r, then $(x - \alpha)^r$ is the highest power of $(x - \alpha)$ that divides f(x) in K[x]. But $\bar{\phi}\left((x - \alpha)^r\right) = (x - \beta)^r$ and $\bar{\phi}\left(f(x)\right) = f(x)$. So β has multiplicity of at least r. A symmetric argument gives the inequality in reverse, so the multiplicity of β equals r.

Corollary 3.10. If K is the splitting field of the polynomial $f(x) \in F[x]$, then f(x) has a factorization in K[x] of the form:

$$f(x) = a(x - \alpha_1)^r(x - \alpha_2)^r \cdots (x - \alpha_n)^r$$

where the α_i's are distinct roots of f(x) in K and $a \in F$.

We need to determine which polynomials have multiple roots. For a polynomial in $\mathbf{R}[x]$, differentiation provides a nice method to answer this question. This method will also serve in arbitrary fields, but first we need to define the derivative of a polynomial over an arbitrary field in a

purely formal way, without refering to limits

Def 3.15: Let $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$. The derivative of $f(x)$ is the polynomial $f'(x)$ where

$$f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}.$$

The mapping $D: F[x] \to F[x]$ defined by $D\big(f(x)\big) = f'(x)$ is rather easily recognizable as a linear transformation. In particular, for $f(x), g(x) \in F[x]$, and $a, b \in F$:

1) $D\big(af(x) + bg(x)\big) = aD\big(f(x)\big) + bD\big(g(x)\big)$

2) $D\big(f(x)g(x)\big) = D\big(f(x)\big)g(x) + f(x)D\big(g(x)\big)$

3) $D(a) = 0$.

Now, we establish a criterion for determining whether a polynomial has multiple roots without knowing the value of the roots.

Thm 3.19: A non-zero polynomial $f(x) \in F[x]$ has a multiple root in the splitting field of $f(x)$ iff $f(x)$ and $f'(x)$ have a non-trivial (i.e. with positive degree) common factor in $F[x]$.

Proof: Let $f(x)$ have a multiple root α in the splitting field of $f(x)$. Then

$f(x) = (x - \alpha)^2g(x)$. This means that

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2g'(x)$$
$$= (x - \alpha)\big(2g(x) + (x - \alpha)g'(x)\big)$$

and $f(x)$ and $f'(x)$ have a common factor, namely $(x - \alpha)$, in $K[x]$. So the minimal polynomial of α over F is a common

factor of $f(x)$ and $f'(x)$ in $F[x]$.

For the only if part of the proof we will use the contrapositive statement. Let $f(x)$ have no multiple roots in K. Then $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where $a \in F$ and the α_i's are all distinct. Then

$$f'(x) = a\sum_{i=1}^{n}(x - \alpha_1) \cdots \overline{(x - \alpha_i)} \cdots (x - \alpha_n),$$

where the $\overline{}$ means the i^{th} factor is deleted. It remains now to be shown that $f(x)$ and $f'(x)$ have no roots on common. If α_i is any root of $f(x)$, consider $f'(\alpha_i)$. $(x - \alpha_i)$ appears as a factor in all but one term of $f'(x)$ Since all the roots of $f(x)$ are distinct, $f'(\alpha_i) \neq 0$. If $f(x)$ and $f'(x)$ have a non-trivial common factor they would have a common root (of the common factor). So $f(x)$ and $f'(x)$ have no non-trivial common factors.

Corollary 3.11: If $f(x) \in F[x]$ is irreducible, then:

1) If char $F = 0$, then $f(x)$ has no multiple roots

2) If char $F = p \neq 0$, then $f(x)$ has a multiple root only if it has the form $f(x) = g(x^p) = a_0 + a_1x^p + \cdots + a_nx^{np}$.

Proof: Let $f(x) \in F[x]$ be irreducible, then the only factors of $f(x)$ in $F[x]$ are a and $f(x)$. If $f(x)$ has a multiple root then $f(x)$ and $f'(x)$ have a non-trivial common factor in $F[x]$. Therefore $f(x) \big/ f'(x)$. But $\deg\big(f'(x)\big) < \deg\big(f(x)\big)$, so $f'(x) = 0$. In a field of characteristic zero, this implies $f(x)$ is constant and therefore has no roots. In case char $F = p \neq 0$, then $f(x) = g(x^p)$.

This corollary does not rule out the possibility that, in a field of non-zero characteristic, an irreducible polynomial might have multiple roots. This leads to many interesting results; which, unfortunately, requires a more sophisticated approach than this paper will attempt. So for the remainder of this study, all fields will be assumed to have charateristic zero unless otherwise noted.

The concept of separability is applied to both polynomials and extensions.

Def 3.16: Let F be a field. An irreducible polynomial in F[x] is called separable iff it has no multiple roots in any extension field of F. An arbitrary polynomial in F[x] is separable iff all of its irreducible factors are separable. Let K:F and $\alpha \in K$ be algebraic over F, then α is separable over F iff its minimal polynomial over F is separable. An algebraic extension K:F is a separable extension iff every $\alpha \in K$ is separable over F. Polynomials, algebraic elements, or algebraic extensions that are not separable are inseparable.

From our discussion earlier concerning multiple roots of irreducible polynomials, it follows that any algebraic extension of a field of characteristic zero is separable.

Def 3.17. A field F is perfect iff all of its algebraic extensions are separable.

A couple of immediate results of this are the following.

Corollary 3.12: Every field of characteristic zero is perfect.

Corollary 3.13: Let F be a field with char F = p ≠ 0 and let f(x) ∈ F[x] be irreducible, then f(x) is not separable iff $f(x) = g(x^p)$ for some g(x) ∈ F[x].

Thm 3.20: Every finite separable extension of a field F is a simple extension.

Proof: Let $E = F(\gamma_1, \ldots, \gamma_n)$ be a finite separable extension of F. We must show there exists a γ ∈ E such that E = F(γ). We shall make the additional assumption that F has infinitely many elements. We will proceed by induction.

Suppose m = 2, so $E = F(\alpha, \beta)$ is a separable extension of F. Let f(x) and g(x) be the minimal polynomials of α and β, respectively, over F. Let K be an extension of F where f(x) and g(x) split. Since E is separable, all roots of f(x) and g(x) are distinct. Let $\alpha_1, \ldots, \alpha_r$ be the roots of f(x) and $\beta_1, \ldots, \beta_s$ be the roots of g(x). So

$f(x) = \prod_{i=1}^{r}(x - \alpha_i)$ and $g(x) = \prod_{j=1}^{s}(x - \beta_j)$.

Consider the $r(s - 1)$ linear equations

$$\alpha_i + y\beta_j = \alpha_1 + y\beta_1 \quad (i = 1, \ldots, r;\ j = 2, \ldots, s)$$

Each equations has at most one solution y in F. Since we assumed F is infinite, we can find a $c \in F$ where c is distinct from all the solutions to our equations. So

$$\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1 \quad (i = 1, \ldots, r;\ j = 2, \ldots, s)$$

We claim that $\gamma = \alpha_1 + c\beta_1 = \alpha + c\beta$ and hence $F(\alpha, \beta) = F(\gamma)$. Clearly γ is in $F(\alpha, \beta)$ since $c \in F$. We have $g(\beta) = 0$ and $f(\gamma - c\beta) = f(\alpha) = 0$. Therefore β is a common root of the polynomials $g(x)$ and $f(\gamma - cx)$. It is the only common root since substituting any other root $\beta_2, \ldots, \beta_s$ of $g(x)$ for x in $f(\gamma - cx)$ is not zero, for by construction $\gamma - c\beta_k \neq \alpha_i$ for $k = 2, \ldots, s$. Since β is a simple root of $g(x)$, the greatest common divisor of $g(x)$ and $f(\gamma - cx)$ is $(x - \beta)$. $g(x)$ and $f(\gamma - cx)$ are both polynomials in $F(\gamma)[x]$. The Euclidean Algorithm tells us that $x - \beta \in F(\gamma)[x]$. Therefore $\beta \in F(\gamma)$ and so is $\alpha = \gamma - c\beta \in F(\gamma)$. So $F(\alpha, \beta) = F(\gamma)$.

To complete the proof we must show $F(\gamma_1, \ldots, \gamma_n) = F(\gamma)$. Assume $F(\gamma_1, \ldots, \gamma_{n-1}) = F(\gamma')$ is simple, then

$$F(\gamma_1, \ldots, \gamma_{n-1}, \gamma_n) = F(\gamma', \gamma_n) = F(\gamma).$$

Corollary 3.14: If F is a field of characteristic zero and if $\gamma_1, \ldots, \gamma_n$ are algebraic over F, then there exists a $\gamma \in F(\gamma_1, \ldots, \gamma_n)$ such that $F(\gamma_1, \ldots, \gamma_n) = F(\gamma)$.

Example: Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. If we let $\gamma = \sqrt{2} + \sqrt{3}$, so $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$. So $\sqrt{2}$ and $\sqrt{3}$ can be written as a linear combination of γ and γ^3, namely $\sqrt{2} = -\frac{9}{2}\gamma + \frac{1}{2}\gamma^3$ and $\sqrt{3} = \frac{11}{2}\gamma - \frac{1}{2}\gamma^3$. Therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Thm 3.21: Let L:K be a separable extension and M an intermediate field, then M:K and L:M are separable.

Proof: M:K is separable, since any multiple roots that showed up in M would also show up in L.

Let $\alpha \in L$ and let $m_1(x)$ be the minimal polynomial of α over M and $m_2(x)$ be the minimal polynomial of α over K. Let N:M be the splitting field for $m_2(x)$ over M. Since $m_2(x)$ is separable over K, it factors as

$$m_2(x) = (x - \alpha_1) \cdots (x - \alpha_r), \text{ where}$$

$\alpha_1, \ldots, \alpha_r$ are distinct elements of N. But $m_1(x) \big/ m_2(x)$ in M[x], so $m_1(x) = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_s})$ where each $\alpha_{i_j} \in \{\alpha_1, \ldots, \alpha_r\}$, and all α_{i_j} are distinct, therefore $m_1(x)$ is separable and L:M is separable.

Thm 3.22: Let L:K be a finite separable extension of degree n. Then there are exactly n distinct K-monomorphisms of L into a normal closure N of L.

Proof: We will use induction on [L:K]. If [L:K] = 1, then the identity is the only one.

Let [L:K] = k > 1, and let $\alpha \in L$, $\alpha \notin K$ with minimal polynomial p(x) over K. $\deg(p(x)) = [K(\alpha):K] = r > 1$. p(x)

is a separable irreducible polynomial with one zero in the normal closure N, so p(x) splits in N and its zero's $\alpha_1, \ldots, \alpha_r$ are distinct. By induction there are precisely s distinct K(α)-monomorphisms $\rho_1, \ldots, \rho_s$: L $\rightarrow$ N where $s = [L:K(\alpha)] = \frac{k}{r}$. There are r distinct K-automorphisms $\tau_1, \ldots, \tau_r$ of N such that $\tau_i(\alpha) = \alpha_i$. The composition maps $\phi_{ij} = \tau_i\rho_j$ gives rs = k distinct K-monomorphisms L $\rightarrow$ N. Let τ: L $\rightarrow$ N be any K-monomorphism. $\tau(\alpha)$ is a zero of p(x) in N, so $\tau(\alpha) = \alpha_i$ for some i. The map $\phi = \tau_i^{-1}\tau$ is a K(α)-monomorphism L $\rightarrow$ N and so $\phi = \rho_j$ for some j. So $\tau = \tau_i\rho_j = \phi_{ij}$ and there are exactly k K-monomorphisms of L $\rightarrow$ N.

CHAPTER 4

Fundamental Theorem of Galois Theory

The basic idea of Galois Theory is to relate a field extension L:K to the group of automorphisms of L that fix each element of K. This chapter will present the Fundamental Theorem of Galois Theory, which states there exists a one-to-one correspondence between the intermediate fields of a separable normal extension L:K of finite degree and the subgroups of the group of automorphisms of L that fix K elementwise. This theorem allows us to translate problems and properties of fields, polynomials, and field extensions into problems in group theory, which are often easier to solve.

We will again define the concept of a K-automorphism and then show that the K-automorphisms of L form a group under the operation of composition of mappings.

Def 4.1: Let K be a subfield of a field L. A K-automorphism of L is an automorphism $\phi: L \to L$ such that $\phi(k) = k$, for all $k \in K$.

Thm 4.1: If L:K is a field extension, then the set of K-automorphisms of L form a group under composition of mappings.

Proof: Associativity follows from the fact that composition of mappings is always associative, and the

identity automorphism is obviously a K-automorphism, so we need to establish closure and inverses.

Let σ and ϕ be K-automorphisms of L. $\sigma\phi$ is an automorphism of L Let $k \in K$, then $\sigma\phi(k) = \sigma(k) = k$, so $\sigma\phi$ is a K-automorphism of L. Also σ^{-1} is an automorphism and for any $k \in K$, $k = \sigma^{-1}\sigma(k) = \sigma^{-1}(k)$, so σ^{-1} is a K-automorphism of L.

Def 4.1: The Galois group, $\Gamma(L:K)$, of the extension L:K is the group of K-automorphisms of L, under composition of mappings.

Examples.

1) Consider $\mathbb{C}:\mathbb{R}$. The only automorphisms of $\mathbb{C}$ that fix $\mathbb{R}$ are the identity and complex conjugation,

$\sigma_1(x + yi) = x + yi$

$\sigma_2(x + yi) = x - yi$,

so $\Gamma(\mathbb{C}:\mathbb{R})$ is the cyclic group of order 2.

2) Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}$. The automorphisms that fix $\mathbb{Q}$ are: ν_1, which is the identity

$\nu_2(\sqrt{2}) = -\sqrt{2}$ $\quad$ $\nu_2(\sqrt{3}) = \sqrt{3}$

$\nu_3(\sqrt{2}) = \sqrt{2}$ $\quad$ $\nu_3(\sqrt{3}) = -\sqrt{3}$

$\nu_4(\sqrt{2}) = -\sqrt{2}$ $\quad$ $\nu_4(\sqrt{3}) = -\sqrt{3}$

The Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}$ is of order 4 and isomorphic to the Klein 4-group.

If M is a field such that $K \subseteq M \subseteq L$, then we have the

Galois groups $\Gamma(L:M)$ and $\Gamma(L:K)$. Since each M-automorphism of L is a K-automorphism of L, $\Gamma(L:M) \leq \Gamma(L:K)$ In the remainder of the paper for each intermediate field M of L:K, we will denote $\Gamma(L:M)$ by M^*. With this notation if $K \subseteq M \subseteq N \subseteq L$, then $N^* \subseteq M^*$. Clearly K^* is the entire Galois group and L^* is the identity subgroup. Conversely, let H be any subgroup of $\Gamma(L:K)$. With H we can associate the set of elements $x \in L$ where $\sigma(x) = x$ for all $\sigma \in H$. We will denote this set by:

$$H^\dagger = \{x \in L \ / \ \sigma(x) = x, \text{ for all } \sigma \in H\},$$

i.e., $H^\dagger$ is the set of all elements of L that are not moved by any element of H. First we will show that $H^\dagger$ is a subfield of L.

Thm 4.2: If H is a subgroup of $\Gamma(L:K)$, then $H^\dagger$ is a subfield of L containing K.

Proof: Associativity, commutativity, and the distributive property are inherited from L. Since 0 and 1 are in K, they are fixed by every element in $\Gamma(L:K)$ and thus are fixed by every element in H. Let $a \in H^\dagger$ and $\sigma \in H$,

$$0 = \sigma(0) = \sigma\big((a + (-a)\big) = \sigma(a) + \sigma(-a) = a + \sigma(-a),$$

so $\sigma(-a) = -a$, and $-a \in H^\dagger$. Similarly for all $a \neq 0 \in H^\dagger$, $a^{-1} \in H^\dagger$. Finally we need to show closure, which is rather easy since $\sigma \in H$ is a morphism.

Let $x, y \in H^\dagger$ and $\sigma \in H$.

$$\sigma(x + y) = \sigma(x) + \sigma(y) = x + y,$$

so $x + y \in H^{\dagger}$. Similarly, $xy \in H^{\dagger}$. Therefore $H^{\dagger}$ is a subfield of L. Since $\sigma \in \Gamma(L:K)$, $\sigma(k) = k$ for all $k \in K$, and $K \subseteq H^{\dagger}$

Example: The Galois group for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}$ is the Klein 4-group $(\nu_1 = 1, \nu_2, \nu_3, \nu_4)$. A subgroup of $\Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q})$ is $S = (\nu_1, \nu_2)$. So $S^{\dagger}$ is the subset of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ not moved by ν_2. These are elements of the form $a + b\sqrt{3}$ Therefore $S^{\dagger} = \mathbb{Q}(\sqrt{3})$.

Def 4.2: If H is a subgroup of $\Gamma(L:K)$, then $H^{\dagger}$ is called the fixed field of H.

It is the relationship between the intermediate fields of the extension L:K and the subgroups of the Galois group $\Gamma(L:K)$ that we wish to examine. We will do this by introducing the concept of a Galois connection between partially ordered sets (we are assuming the reader is familiar with this concept).

Def 4.3: Let $(P, \leq)$ and $(Q, \leq^*)$ be partially ordered sets. A Galois connection between P and Q is a pair of mappings, $\sigma: P \to Q$ and $\tau: Q \to P$, satisfying:

1) if $p_1 \leq p_2$ $p_1, p_2 \in P$, then $\sigma(p_2) \leq^* \sigma(p_1)$

2) if $q_1 \leq^* q_2$ $q_1, q_2 \in Q$, then $\tau(q_2) \leq \tau(q_1)$

3) $p \leq \tau\sigma(p)$ $\forall\ p \in P$

4) $q \leq^{*} \sigma\tau(q) \quad \forall\ q \in Q$.

So σ and τ are order-reversing and extensive mappings

In our case, the set of intermediate fields of an extension and the set of subgroups of the Galois group of the extension are partially ordered by set inclusion.

Thm 4.3. Let P be the set of all intermediate fields of the field extension L:K. Let Q be the set of all subgroups of the Galois group $\Gamma(L:K)$. Define σ: $P \to Q$ and τ: $Q \to P$ by

$\sigma(F) = \{ \psi \in \Gamma(L:K) \ / \ \psi(a) = a \quad \forall\ a \in F \}$, where $F \in P$,

and

$\tau(H) = \{ a \in L \ / \ \psi(a) = a \quad \forall \in H \}$, where $H \in Q$.

That is, $\sigma(F) = F^{*}$ and $\tau(H) = H^{\dagger}$.

Then σ and τ define a Galois connection betwee P and Q.

Proof: Let P and Q be as defined above and σ and τ also.

1) Let $K \subseteq P_1 \subseteq P_2 \subseteq L$. Let $\gamma \in \sigma(P_2)$. Since γ fixes everything in P_2 and $P_1 \subseteq P_2$, γ fixes everything in P_1 and $\gamma \in \sigma(P_1)$ So $\sigma(P_2) \subseteq \sigma(P_1)$.

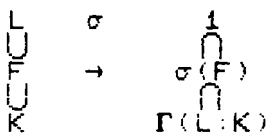
2) Let Q_1, $Q_2 \in Q$ and $Q_1 \subseteq Q_2$. Let $a \in \tau(Q_2)$. a is fixed by every element in Q_2 and since Q_1 is contained in Q_2, a is fixed by every element in Q_1, and $a \in \tau(Q_1)$. So $\tau(Q_2) \subseteq \tau(Q_1)$.

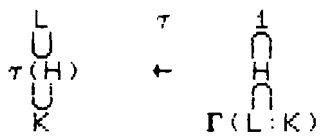
3) Let $F \in P$ and $a \in F$. $\gamma(a) = a$ for all $\gamma \in \sigma(F)$ $\tau\sigma(F)$ is all $a \in L$, where $\gamma(a) = a$ for all $\gamma \in \sigma(F)$, so

$a \in \tau\sigma(F)$ and $F \subseteq \tau\sigma(F)$.

4) Let $H \in Q$. $\tau(H)$ is the fixed field of H. So every $\gamma \in H$ will fix every element in $\tau(H)$. $\sigma\tau(H)$ is all automorphisms that fix $\tau(H)$ and so must contain γ. So $H \subseteq \sigma\tau(H)$, and our theorem is proved.

We have the relationship pictured below (1 is the identity subgroup of $\Gamma(L:K)$).





If we apply σ to L and K and τ to 1, the results are rather obvious. $\sigma(L) = 1$, $\sigma(K) = \Gamma(L:K)$, and $\tau(1) = L$. But $\tau(\Gamma(L:K))$ may be larger than K. We are interested in when $\tau(\Gamma(L\ K)) = K$. Having a normal extension of a field of characteristic zero will do the trick (Kaplansky defines normal extensions as: given $\alpha \in L$ but $\alpha \notin K$ there exists an automorphism fixing K but moving α). To prove the Fundamental Theorem of Galois Theory we need some preliminary theorems relating the order of the subgroup to the degree of the field extension. We will start with a theorem due to Dedekind.

Thm 4.4: If K and L are fields, then every set of distinct monomorphisms from K to L is linearly independent over L.

Proof: Let $\lambda_1, \ldots, \lambda_n$ be distinct monomorphisms $K \to L$.

Assume there exists $a_1, \ldots, a_n \in L$, not all zero and n is the minimum value, such that

(1) $a_1\lambda_1(x) + \ldots + a_n\lambda_n(x) = 0$ for all $x \in K$

We may assume that $a_i \neq 0$ for all $i = 1, \ldots, n$. There exists a $y \in K$ such that $\lambda_1(x) \neq \lambda_n(x)$ since the λ's are distinct. Therefore $y \neq 0$. Since $yx \in K$,

$a_1\lambda_1(yx) + \ldots + a_n\lambda_n(yx) = 0$ or

(2) $a_1\lambda_1(y)\lambda_1(x) + \ldots + a_n\lambda_n(y)\lambda_n(x) = 0$.

Multiplying (1) by $\lambda_1(y)$ and subtracting (2) we obtain,

$$a_2\big(\lambda_2(x)\lambda_1(y) - \lambda_2(x)\lambda_2(y)\big) + \ldots + a_n\big(\lambda_n(x)\lambda_1(y) - \lambda_n(x)\lambda_n(y)\big) = 0.$$

The coefficient of $\lambda_n(x)$ is $a_n\big(\lambda_1(y) - \lambda_n(y)\big)$ and since $\lambda_1(y) - \lambda_n(y) \neq 0$ we have an expression with fewer terms than (1), which contradicts the assumption of n as least value. Therefore $\lambda_1, \ldots, \lambda_n$ are linearly independent.

Thm 4 5. Let H be a finite subgroup of the group of automorphisms of a field K, and let $H^\dagger$ be the fixed field of H. then $[K:H^\dagger] = |H|$.

Proof: Let $n = |H|$ and $H = \{g_1, \ldots, g_n\}$ where $g_1 = 1$

Part I: Suppose $[K:H^\dagger] = m > n$. Let $\{x_1, \ldots, x_m\}$ be a basis for K over $H^\dagger$ By a well-known theorem from linear algebra we can find $y_1, \ldots y_n \in K$, not all zero such that,

$g_1(x_j)y_1 + \ldots + g_n(x_j)y_n = 0$ for $j = 1, \ldots, m$.

Let $a \in K$. then $a = \alpha_1x_1 + \ldots + \alpha_mx_m$, where $\alpha_1, \ldots, \alpha_m \in H^\dagger$. So

$$g_1(a)y_1 + \ldots + g_n(a)y_n = g_1\Big(\sum_i \alpha_i x_i\Big)y_1 + \ldots + g_n\Big(\sum_i \alpha_i x_i\Big)y_n$$

$$= \sum_i \alpha_i \left(g_1(x_i)y_1 + \ldots + g_n(x_i)y_n \right) = 0$$

Therefore $g_1, \ldots, g_n$ are linearly dependent contrary to Dedekind's Theorem. Therefore $m \leq n$.

Part II: Suppose $[K:H^\dagger] > n$. Then there exists $x_1, \ldots, x_{n+1} \in K$ linearly independent over $H^\dagger$. By the previous well-known theorem from linear algebra, there exists $y_1, \ldots, y_{n+1} \in K$ not all zero, such that for $j = 1, \ldots, n$

$$g_j(x_1)y_1 + \ldots + g_j(x_{n+1})y_{n+1} = 0.$$

Let us deal strictly with the non-zero y_i's and renumber so $y_1, \ldots, y_r \neq 0$ and $y_{r+1}, \ldots, y_{n+1} = 0$, so

$$(1) \quad g_j(x_1)y_1 + \ldots + g_j(x_r)y_r = 0$$

Let $g \in H$ and operate on (1) with g. We get the system.

$$gg_j(x_1)g(y_1) + \ldots + gg_j(x_r)g(y_r) = 0.$$

As j varies from 1 to n (by a well-known theorem from group theory) this system is equivalent to

$$(2) \quad g_j(x_1)g(y_1) + \ldots + g_j(x_r)g(y_r) = 0$$

Multiply (1) by $g(y_1)$ and (2) by y_1 and subtract, getting.

$$g_j(x_2)\left(y_2g(y_1) - g(y_2)y_1\right) + \ldots + g_j(x_r)\left(y_rg(y_1) - g(y_r)y_1\right) = 0.$$

This has fewer terms than (1) and contradicts the fact that r was choosen to be the least value. Thus we must have each $y_ig(y_1) - g(y_i)y_1 = 0$. However, in that case $y_iy_1^{-1} = g(y_iy_1^{-1})$ and $y_iy_1^{-1} \in H^\dagger$. So there exists $z_1, \ldots, z_r \in H^\dagger$ and $k \in K$, $k \neq 0$ such that $y_i = kz_i$ for all i. With $j = 1$, (1) becomes,

$$x_1kz_1 + \ldots + x_rkz_r = 0.$$

Dividing by k we get a linearly dependent basis. So $[K:H^{\dagger}] \leq n$.

Therefore $[K:H^{\dagger}] = |H|$.

Corollary 4.1: If $\Gamma(L:K)$ is the Galois group of the finite extension L:K and H is a finite subgroup of $\Gamma(L:K)$, then $[H^{\dagger}:K] = [L:K]/|H|$.

Proof: $[L:H^{\dagger}][H^{\dagger}:K] = [L:K]$, so

$$[H^{\dagger}:K] = [L:K]/[L:H^{\dagger}] = [L:K]/|H|.$$

The proof of the last two parts of the Fundmental Theorem of Galois Theory will require the following lemma.

Lemma 1: Let L:K be a finite, separable, normal extension, M an intermediate field, and $\lambda \in \Gamma(L:K)$; then $\sigma(\lambda(M)) = \lambda(\sigma(M))\lambda^{-1}$.

Proof: Let $\gamma \in \sigma(M)$ and $x_1 \in \lambda(M)$. Therefore $x_1 = \lambda(x)$ for some $x \in M$. So,

$$(\lambda\gamma\lambda^{-1})(x_1) = (\lambda\gamma)(x) = \lambda(x) = x_1, \text{ so}$$

$$\lambda(\sigma(M))\lambda^{-1} \subseteq \sigma(\lambda(M)).$$

Let $x \in M$ and $x_0 = \lambda(x)$, then

$$(\lambda^{-1}\gamma\lambda)(x) = \lambda^{-1}\gamma(x_0) = \lambda^{-1}(x_0) = x, \text{ so}$$

$$\lambda^{-1}(\sigma(\lambda(M)))\lambda \subseteq \sigma(M).$$

Multiplying on the right by λ^{-1} and on the left by λ we get $\sigma(\lambda(M)) \subseteq \lambda(\sigma(M))\lambda^{-1}$, and the equality holds.

We now have the pieces necessary to establish the Fundamental Theorem of Galois Theory.

Thm 4.6. (Fundamental Theorem of Galois Theory) Let L be a field of characteristic zero that is a finite normal extension of a field K. Let $\Gamma(L:K)$ be the Galois group of L over K. Let P be the set of intermediate fields between L and K and let Q be the set of subgroups of $\Gamma(L:K)$. Define $\sigma: P \to Q$ and $\tau: Q \to P$ where:

$\sigma(M) = \Gamma(L:M)$ for all $M \in P$, and

$\tau(H) = \{a \in L \mid \psi(a) = a \text{ for all } \psi \in H\}$ for all $H \in Q$

Then:

1) $|\Gamma(L:K)| = [L:K]$

2) $\tau\sigma(M) = M$ and $\sigma\tau(H) = H$

3) If $K \subseteq M \subseteq L$, then $[L:M] = |\sigma(M)|$ and

$[M:K] = |\Gamma(L:K)|/|\sigma(M)|$

4) An intermediate field M is a normal extension of K if and only if $\sigma(M)$ is a normal subgroup of $\Gamma(L:K)$.

5) If an intermediate field M is a normal extension of K then the Galois group of M:K is isomorphic to $\frac{\Gamma(L:K)}{\sigma(M)}$.

Proof: 1) Since L:K is finite, normal, and separable there are precisely n distinct K-automorphisms of L, where $n = [L:K]$, so $|\Gamma(L:K)| = n$.

2) Let M be an intermediate field of L:K. L:M is separable and normal. Let $M^{\dagger}$ be the fixed field of $\Gamma(L:M)$. $[L:M^{\dagger}] = |\Gamma(L:M)|$. But $[L:M] = |\Gamma(L:M)|$.

Since $M \subseteq \tau\sigma(M) = M^{\dagger}$, $M = \tau\sigma(M)$.

Now consider a subgroup H of $\Gamma(L:K)$. We know $H \subseteq \sigma\tau(H)$ From the preceeding argument $\tau(H) = \tau\sigma\tau(H)$. Since $\tau(H)$ is the fixed field of H, $|H| = [L:\tau(H)]$, which implies $|H| = [L\ \tau\sigma\tau(H)]$. Since $\tau\sigma\tau(H)$ is the fixed field of $\sigma\tau(H)$, $[L:\tau\sigma\tau(H)] = |\sigma\tau(H)|$. So $|H| = |\sigma\tau(H)|$ and since these are finite groups, $H = \sigma\tau(H)$.

3) Again L:M is separable, finite, and normal, so $[L:M] = |\Gamma(L:M)| = |\sigma(M)|$ and the second follows from Corollary 4.1.

4) Let M be an intermediate field of L:K and let M:K be a normal extension. Let $\gamma \in \Gamma(L:K)$. Then $\gamma|_M$ is a K-monomorphism $M \to L$ and is therefore a K-automorphism of M. So $\gamma(M) = M$ and by Lemma 1, $\gamma\big(\sigma(M)\big)\gamma^{-1} = \sigma(M)$ and $\sigma(M)$ is a normal subgroup of $\Gamma(L:K)$.

Let $\sigma(M)$ be a normal subgroup of $\Gamma(L:K)$ and let γ be any K-monomorphism $M \to L$. We know there exists a K-automorphism λ of L such that $\lambda|_M = \gamma$. Since $\sigma(M)$ is a normal subgroup, $\lambda\big(\sigma(M)\big)\lambda^{-1} = \sigma(M)$ and by Lemma 1, $\sigma\big(\lambda(M)\big) = \sigma(M)$ By part 2) of this theorem, $\lambda(M) = M$. This means $\gamma(M) = M$ and γ is a K-automorphism of M. Hence M:K is a normal extension.

5) Let M be an intermediate field of L:K and M:K be a normal extension. Let $G = \Gamma(L:K)$ and $G' = \Gamma(M:K)$. Define a map ϕ: $G \to G'$ by $\phi(\gamma) = \gamma|_M$ for all $\gamma \in G$. Since $\gamma|_M$ is a K-automorphism of M, ϕ will preserve the operation of composition of mappings and is a homomorphism. The identi-

ty for G' is the identity mapping on M, so ker ϕ will be those $\gamma \in G$ that fix M. In other words ker $\phi = \Gamma(L\ M)$ By the First Fundamental Theorem of Group Homomorphisms, $G' \simeq \frac{G}{\sigma(M)}$.

Examples: 1) Let K = $\mathbb{Q}$ and let L be the extension field of $\mathbb{Q}$ formed by the adjunction of the seventeenth roots of unity. L is the splitting field over $\mathbb{Q}$ of $f(x) = x^{17} - 1$. Since $f(x)$ and $f'(x) = 17x^{16}$ have no non-trivial factors in common, all the roots of $x^{17} - 1$ are distinct. $x^{17} - 1$ will factor in $\mathbb{Q}$ to $(x - 1)(x^{16} + x^{15} + \ldots + x + 1)$. If we let z be the primitive seventeenth root of unity, then $L = \mathbb{Q}(z)$. The irreducible polynomial $x^{16} + x^{15} + \ldots + x + 1$ is the minimal polynomial of z over $\mathbb{Q}$ and $[\mathbb{Q}(z):\mathbb{Q}] = 16 = |\Gamma(\mathbb{Q}(z)\ \mathbb{Q})|$ $f(x)$ is the 17th cyclotomic polynomial, Φ_{17}, and its Galois group is cyclic. Thus $\Gamma(\mathbb{Q}(z):\mathbb{Q}) = \{ \gamma, \gamma^2, \ldots, \gamma^{16} = 1\}$ and we have the chain of subgroups:

$$\Gamma(\mathbb{Q}(z):\mathbb{Q}) = \langle\gamma\rangle \supset G_2 = \langle\gamma^2\rangle \supset G_3 = \langle\gamma^4\rangle \supset G_4 = \langle\gamma^8\rangle \supset G_5 = (1)$$

The respective orders are 16, 8, 4, 2, and 1 The Galois Connection gives us a sequence of subfields:

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset F_4 \subset F_5 = \mathbb{Q}(z),$$

where each F_i corresponds to G_i in the Galois Connection. There are, therefore, exactly three intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(z)$. Since the Galois group is abelian all of its subgroups are normal, therefore every subfield of $\mathbb{Q}(z)$ is normal over $\mathbb{Q}$.

2) Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, and let L be the splitting field for f over $\mathbb{Q}$. $f(x)$ factors as:

$(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$, where $\sqrt[4]{2} \in \mathbb{R}^+$ and $i = \sqrt{-1}$. Therefore $L = \mathbb{Q}(\sqrt[4]{2}, i)$. For ease of notation let $\zeta = \sqrt[4]{2}$, so $L = \mathbb{Q}(\zeta, i)$. To calculate the degree of $\mathbb{Q}(\zeta, i)$ $\mathbb{Q}$ we note: $[\mathbb{Q}(\zeta, i):\mathbb{Q}] = [\mathbb{Q}(\zeta, i):\mathbb{Q}(\zeta)]\,[\mathbb{Q}(\zeta):\mathbb{Q}]$.

The minimal polynomial of i over $\mathbb{Q}(\zeta)$ is $x^2 + 1$. Since $x^2 + 1$ has no roots in $\mathbb{Q}(\zeta)$, it is irreducible over $\mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta, i):\mathbb{Q}(\zeta)] = 2$. By Eisenstein's criterion for irreducibility with $p = 2$, $x^4 - 2$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\zeta):\mathbb{Q}] = 4$. This gives $[\mathbb{Q}(\zeta, i):\mathbb{Q}] = 2 \cdot 4 = 8$ and the order of the Galois group $\Gamma(\mathbb{Q}(\zeta, i):\mathbb{Q})$ is 8.

The Galois group will be generated by the two automorphisms σ and τ where:

$\sigma(i) = i \qquad \sigma(\zeta) = i\zeta$

$\tau(i) = -i \qquad \tau(\zeta) = \zeta$

These two generators yield the following $\mathbb{Q}$-automorphisms

automorphisms	$\zeta \mapsto$	$i \mapsto$
1	ζ	i
σ	$i\zeta$	i
σ^2	$-\zeta$	i
σ^3	$-i\zeta$	i
τ	ζ	$-i$
$\sigma\tau$	$i\zeta$	$-i$
$\sigma^2\tau$	$-\zeta$	$-i$
$\sigma^3\tau$	$-i\zeta$	$-i$

$\Gamma(\mathbb{Q}(\zeta, i):\mathbb{Q})$ can be expressed in terms of generators and relations by $\Gamma(\mathbb{Q}(\zeta, i):\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^3 = \sigma^{-1} \rangle$, which is isomorphic to the dihedral group of order 8, $\mathcal{D}_4$.

The subgroups of $\mathcal{D}_4$ are as follows:

$\mathcal{D}_4$

order 4: $A = \{1, \sigma, \sigma^2, \sigma^3\}$

$B = \{1, \sigma^2, \tau, \sigma^2\tau\}$

$C = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$

order 2: $D = \{1, \sigma^2\}$

$E = \{1, \tau\}$

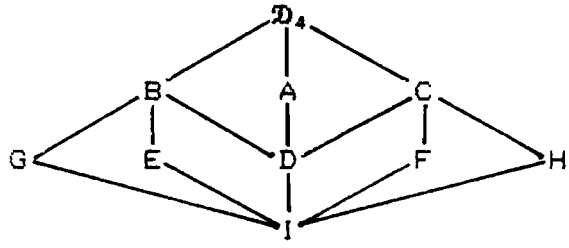
$F = \{1, \sigma\tau\}$

$G = \{1, \sigma^2\tau\}$

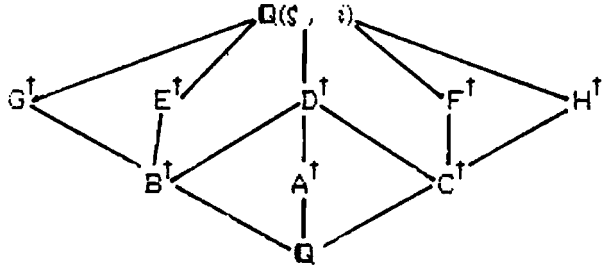
$H = \{1, \sigma^3\tau\}$

order 1: $I = \{1\}$

The lattice of subgroups is given by:



The corresponding tower of subfields is given by:



There are three subfields of $\mathbb{Q}(\zeta, i)$ of degree 2 over $\mathbb{Q}$.

They are the splitting fields of the irreducible polynomials $x^2 + 1$, $x^2 + 2$, $x^2 - 2 \in \mathbb{Q}[x]$. They are $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$, and $\mathbb{Q}(\sqrt{2})$, and they are fixed by $A^\dagger$, $C^\dagger$, and $B^\dagger$ respectively. The fields $G^\dagger$, $E^\dagger$, $D^\dagger$, $F^\dagger$, and $H^\dagger$ can be calculated in the following manner.

If $x \in \mathbb{Q}(\zeta, i)$, then:

$$x = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4 i + a_5 i\zeta + a_6 i\zeta^2 + a_7 i\zeta^3,$$

where $a_i \in \mathbb{Q}$. Consider $E^\dagger$. It is the field fixed by $(1, \tau)$.

$$\tau(x) = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 - a_4 i - a_5 i\zeta - a_6 i\zeta^2 - a_7 i\zeta^3.$$

Therefore $a_0, \ldots, a_3$ are arbitrary and $a_4, \ldots, a_7 = 0$, so

$$x = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3, \text{ and } E^\dagger = \mathbb{Q}(\zeta).$$

Similarly we can find $G^\dagger = \mathbb{Q}(i\zeta)$, $D^\dagger = \mathbb{Q}(\sqrt{2}, i)$, $F^\dagger = \mathbb{Q}(\zeta(1 + i))$, and $H^\dagger = \mathbb{Q}(\zeta(1 - i))$.

The normal subgroups of $\mathfrak{D}_4$ are $\mathfrak{D}_4$, A, B, C, D, and I, so the corresponding subfields $\mathbb{Q}$, $A^\dagger$, $B^\dagger$, $C^\dagger$, $D^\dagger$, and $\mathbb{Q}(\zeta, i)$ are the only normal extensions of $\mathbb{Q}$. These are the splitting fields of x, $x^2 - 2$, $x^2 + 2$, $x^4 - x^2 - 2$, $x^4 - 2$, respectively.

According to part 5 of the Fundamental Theorem of Galois Theory, since $D^\dagger$ is a normal extension of $\mathbb{Q}$ the Galois group of $D^\dagger:\mathbb{Q}$ is isomorphic to $\frac{\Gamma(\mathbb{Q}(\zeta, i):\mathbb{Q})}{D}$. The $\mathbb{Q}$-automorphisms of $D = \mathbb{Q}(\sqrt{2}, i)$ are $\{1, \alpha, \beta, \alpha\beta\}$, where $\alpha(i) = i$, $\alpha(\sqrt{2}) = -\sqrt{2}$, $\beta(i) = -i$, $\beta(\sqrt{2}) = \sqrt{2}$, $\alpha\beta(i) = -i$, $\alpha\beta(\sqrt{2}) = -\sqrt{2}$. The quotient group $\frac{\Gamma(\mathbb{Q}(\zeta, i):\mathbb{Q})}{D}$ contains the cosets $\{(1, \sigma^2), (\sigma, \sigma^3), (\tau, \sigma^2\tau), (\sigma\tau, \sigma^3\tau)\}$. We have the isomorphism:

$$1 \leftrightarrow (1, \sigma^2)$$

$\alpha \quad \mapsto \quad (\sigma, \ \sigma^3)$

$\beta \quad \mapsto \quad (\tau, \ \sigma^2\tau)$

$\alpha\beta \quad \mapsto \quad (\sigma\tau, \ \sigma^3\tau)$

So both of these groups are isomorphic to the Klein 4-group or $\mathbb{C}_2 \otimes \mathbb{C}_2$.

The Galois connection between the lattice of subgroups and the tower of subfields can be seen graphically if either one is inverted.

Summary

Through the Fundamental Theorem of Galois Theory the problem of solvability of polynomials can be looked at from the view of group theory rather than the more difficult standpoint of field theory. We have seen that, starting with a polynomial p(x) irreducible over a field F, a splitting field E exists. This splitting field is a finite normal extension of F. If F has characteristic zero, then for every subgroup of the Galois group of the extension E:F there exists a intermediate subfield of E. Conversely, for every intermediate subfield between E and F there exists a subgroup of the Galois group of E:F which fixes the intermediate field.

In this paper we have not attempted to answer the question of whether a polynomial is solvable by radicals. To answer that question, one needs to examine the structure of the

Galois group of the splitting field of the polynomial over the base field. If the Galois group is solvable then the polynomial is solvable by radicals. By showing the existence of a fifth degree polynomial which has as a Galois group S_5, which is not solvable, the quintic is seen to be not solvable by radicals. This did not stop the search for a solution to the general fifth degree polynomial equation. Jerrard in 1834 was able to show that the quintic is solvable by radicals and ultraradicals, where the ultraradical $\sqrt[*]{a}$ is defined to be the real root of $x^5 + x - a$. Hermite (1822-1902) was able to solve the quintic using elliptic modular functions, which arose in the context of integration of algebraic functions. The connection Galois found between the subgroups and subfields was generalized and applied in many different areas of mathematics. The idea of a Galois connection has been applied to commutative rings, division rings, and differential equations. Each of these areas has its own Fundamental Theorem corresponding to the Fundamental Theorem of this paper.

The problem of solving a polynomial equation has occupied many of the most brilliant mathematicians since Cardano first published the solution to the cubic and quartic equations. It is a problem which continues to generate much in the way of "good" mathematics.

BIBLIOGRAPHY

[1] Artin, E., Galois Theory.

Notre Dame Notre Dame Mathematical Lectures, 1942

[2] Bell, E. T., Men of Mathematics.

New York: Simon and Schuster, 1937.

[3] Birkoff, G., MacLane, S., A Survey of Modern Algebra.

New York: The MacMillian Company, 1965.

[4] Boyer, Carl B., A History of Mathematics.

New York: John Wiley & Sons, Inc., 1968.

[5] Deskins, W.E., Abstract Algebra.

New York: The MacMillian Company, 1964.

[6] Gaal, Lisl, Classical Galois Theory with Examples.

New York: Chelsea Publishing Company, 1979.

[7] Garling, D. J. H., A Course in Galois Theory.

Cambridge Cambridge University Press, 1986

[8] Goldstein, Larry Joel, Abstract Algebra.

New Jersey: Prentice-Hall, 1973.

[9] Jacobson, Nathan, Basic Algebra I.
New York: W. H. Freeman and Company, 1985.

[10] Kaplansky, Irving, Fields and Rings.
Chicago: University of Chicago Press, 1965.

[11] McCarthy, Paul, Algebraic Extensions of Fields.
Waltham Mass.: Blaisdell Publishing Company, 1966.

[12] Stewart, Ian, Galois Theory.
London: Chapman and Hall, 1973.