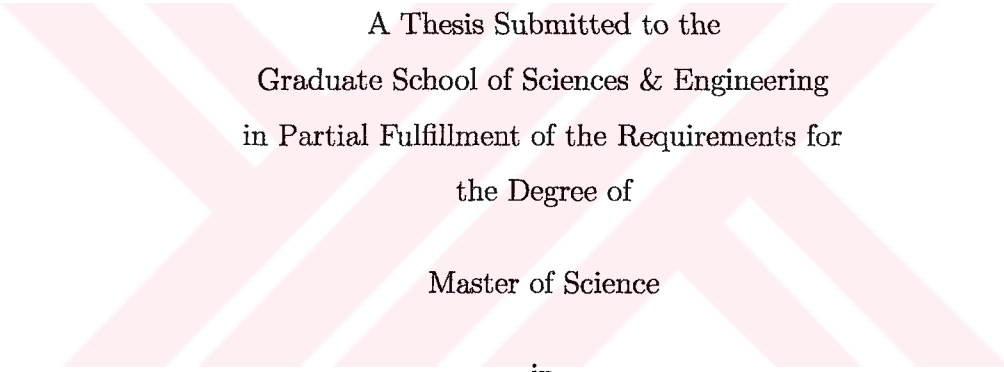


COGALOIS THEORY VERSUS GALOIS THEORY

by

Hatice Boylan



A Thesis Submitted to the
Graduate School of Sciences & Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

Koç University

June, 2005

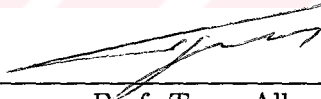
Koç University
Graduate School of Sciences & Engineering

This is to certify that I have examined this copy of a master's thesis by

Hatice Boylan

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:



Prof. Toma Albu



Prof. Oleg Belegradek



Prof. Ali Ülger

Date:

09/05/2005

To my parents



ABSTRACT

Since the middle of the sixteenth century to the beginning of the nineteenth century some of the greatest mathematicians of this period have tried to obtain a formula for the roots of quintic equations. Before that period it was known that the solutions of the equations of degree less than or equal to 4 were expressible by radicals, in other words, the polynomials up to the quartic were solvable by radicals (a radical is a formula involving only the 4 basic arithmetic operations and the extraction of roots). Galois not only solved this important problem which could not be solved for centuries, but he also provided a criterion for solvability by radicals of any equation $x^n + a_{n-1}x^{n-1} + \dots = 0$. Actually, the importance of the main result of Galois' discoveries has transcended by far that of the original problem which lead to it. His discoveries in the theory of equations is called *Galois Theory*. Galois Theory investigates field extensions possessing a *Galois correspondence*. *Cogalois Theory*, a fairly new theory of about 20 years old is dual to the Galois Theory and investigates field extensions possessing a *Cogalois correspondence*.

The main objective of this work is to present the fundamentals of Galois Theory and Cogalois Theory. Firstly, we investigate Galois Theory. We start by providing some concepts in order to define the Galois extensions and the Galois group of a given field extension. Two major results of Galois Theory are given, namely *The Fundamental Theorem of Finite Galois Theory* and *The Galois' Criterion for Solvability by Radicals*. Then we work on Cogalois Theory. In that part we provide some results, such as *The Kneser Criterion* and *The Greither-Harrison Criterion*. Lastly, we define G -Cogalois extensions. A G -Cogalois extension is a separable field extension with G/F^* -Cogalois correspondence. The importance of these extensions stems from the fact that they play the same role as that of Galois extensions in Galois Theory.

ACKNOWLEDGMENTS

I would like to thank my supervisor Prof. Toma Albu for his many suggestions and patience during my research. I was able to take advantage of his deep knowledge and experience. I would also like to express my gratitude to him for his guidance through the process of writing this Thesis in L^AT_EX. I am grateful to Prof. Ali Ülger and Prof. Oleg Belegradek for accepting to be in the thesis committee.

I am grateful to my parents Mustafa Boylan and Resmiye Boylan for their love and support that they always provide. Without their confidence in me this work would never have come into existence. I would also like to thank my sisters for always being there and for their continuous support.

Last, but not least, I am grateful to Utku for his constant encouragement and his stylistic help. I am also thankful to him for the good and hard times we had together.

TABLE OF CONTENTS

Chapter 1:	Preliminaries	7
Chapter 2:	Galois Theory	12
2.1	The Life of Galois	12
2.2	Some Results on Solvable Groups	17
2.3	Basic Field Theory	19
2.4	Ruler and Compass Constructions	36
2.5	Splitting Fields	40
2.6	Foundations of Galois Theory	45
2.6.1	Galois Correspondence	46
2.7	The Galois' Criterion for Solvability by Radicals	61
Chapter 3:	Cogalois Theory	74
3.1	The Vahlen-Capelli Criterion	74
3.2	Some Results on Bounded Abelian Groups	87
3.3	Kneser Extensions	88
3.3.1	G -radical and G -Kneser Extensions	88
3.3.2	The Kneser Criterion	94
3.4	Cogalois Extensions	103
3.4.1	The Greither-Harrison Criterion	103
3.4.2	Some Examples and Properties of Cogalois Extensions	110
3.4.3	The Cogalois Group of a Quadratic Extension	120
3.5	Strongly Kneser Extensions	123
3.5.1	Galois and Cogalois Connections	124

3.5.2	Strongly G -Kneser Extensions	129
3.5.3	G -Cogalois Extensions	136
3.5.4	The Kneser group of a G -Cogalois extension	140
3.5.5	Galois G -Cogalois Extensions	142
3.5.6	Some Examples of G -Cogalois Extensions	144
	Bibliography	155
	Vita	157



INTRODUCTION

In Elementary Algebra the solution

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

to the quadratic equation $ax^2 + bx + c = 0$ was known to the Babylonians around 2000 BC. During the period of the Italian Renaissance the roots of the cubic and the quartic equations were also formulated. The first one was formulated by Scipione Del Ferro (1465-1509) and Niccolo Tartaglia (1499-1557) independently. Tartaglia's solutions were given in terms of root extractions and rational operations. The second one was attributed to Geronimo Cardano's assistant Ludovico Ferarri (1522-1565). His method was similar to the one which was used for cubics.

Although the quartic equation has been solved by radicals in the 1500's, the quintic equation remained a puzzle for the next 300 years. The reason was that most of the mathematicians of this period believed that a formula for the quintic equations would be formulated soon. Joseph-Louis Lagrange obtained considerably better solutions than the other mathematicians who worked on the same problem. He showed that the general method, which was used for proving the solvability of an equation of degree ≤ 4 , did not work when it is tried on the quintic. It did not prove that the quintic was not solvable by radicals, since there might had been another method which would provide a formula for the quintic. But failure of such a general method caused suspicion among people.

In 1799, Paolo Ruffini (1765-1822) published a book on the insolvability of the quintic. But in the mathematical community the proof was thought to be unsatisfactory. There was a gap in the proof. Nonetheless, he had made an improvement for the solution of the problem and he deserved appreciation for it.

The problem remained until 1824 when Niels Henrik Abel (1802-1829) proved that the general quintic equation was not solvable by radicals. He filled in the gap in Ruffini's proof. This achievement lead Abel to work on any particular polynomial of any degree. But he died in 1829 without proving this new problem.

Évariste Galois (1811-1832), a mathematical genius independently proved the insolvability of the quintic using his Galois Theory. The Galois Theory has far-reaching implications than its original purpose, it can be used to determine which equations can be solved and which cannot be solved by radicals.

In his theory, for a finite Galois extension E/F , Galois found that there was a canonical one-to-one, order-reversing correspondence, in other words, a *lattice anti-isomorphism* between the lattice ξ of the set of all subfields of E containing F , and Γ , the lattice of all subgroups of the Galois group $\text{Gal}(E/F)$. Later these extensions are called the *extensions with Γ -Galois correspondence*. With the help of this result, Galois managed to describe the lattice of all intermediate fields of the extension E/F in terms of the lattice of all subgroups of Γ . So, the problem of the solvability of the quintic equation is reduced into a group theoretical one.

There are also finite field extensions which are not necessarily Galois for which there exists a canonical one-to-one, order preserving correspondence, or equivalently, a *lattice isomorphism* between the lattice ξ of all intermediate fields of the extension E/F and the lattice \mathcal{D} of all subgroups of a certain group Δ canonically associated with the extension E/F . These extensions are called *extensions with Δ -Cogalois correspondence*. Cogalois Theory, a fairly new theory, only about 20 years old, investigates these field extensions which are finite or infinite. This theory is dual to the Galois Theory which investigates field extensions possessing a Galois correspondence.

The term "extension with Cogalois correspondence" was introduced by Albu and Nicolae [2] in order to emphasize a situation which is dual to that appearing in Galois Theory.

The term "Cogalois" first appeared in the literature in 1986 in the fundamental paper of Greither and Harrison [9]. In their paper they introduced and investigated

“Cogalois extensions”. Also in 1991 Barrera-Mora, Rzedowski-Calderón and Villa-Salvador published a paper [7] on this subject. In 1986, Greither and Harrison showed that the extension

$$\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q},$$

where $r \in \mathbb{N}^*$, $n_1, \dots, n_r, a_1, \dots, a_r \in \mathbb{N}^*$, and for every $1 \leq i \leq r$, $\sqrt[n_i]{a_i}$ is the positive real n_i -th root of a_i , is an extension with Δ -Cogalois correspondence. The associated group Δ , for this extension is the factor group $\mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle / \mathbb{Q}^*$. So, they obtained

$$[\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r}) : \mathbb{Q}] = |\mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle / \mathbb{Q}^*|.$$

Kneser tried to find an explicit formula in order to compute $[F(x_1, \dots, x_r) : F]$, where $x_1, \dots, x_r \in \overline{F}$ and \overline{F} is an algebraic closure of F . Partial answers were given to this problem, but Kneser in his paper [12], answered this problem for a large class of extensions. These extensions were later called by T. Albu and F. Nicolae [2] Kneser extensions.

In their paper, Greither and Harrison [9] also presented two other large classes of field extensions with Δ -Cogalois correspondence. These are *Cogalois extensions and the neat presentations*. The classical finite Kummer extensions are extensions with Galois and Cogalois correspondences, and the two groups in these correspondences are isomorphic. So, the extensions of type $\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q}$, the Cogalois extensions, the neat presentations, and the finite classical Kummer extensions all are field extensions with Δ -Cogalois correspondence.

Albu and Nicolae [2] investigated separable finite radical extensions with Δ -Cogalois correspondence and continued this subject in [3], [4], [5], [6]. They introduced the concept of G -Cogalois extensions.

This Thesis is divided into two parts: part 1 is devoted to Galois Theory and part 2 is devoted to Cogalois Theory. In Chapter 1, necessary preliminaries are given containing the terminology and notation which are used throughout the Thesis.

Chapter 2 investigates the Galois Theory. We basically follow N. Jacobson [10]

and I. Kaplansky [11] in this chapter. We start this chapter by the life of Galois. Then some results from Group Theory which are needed in the proof of *The Galois' Criterion for Solvability by Radicals* are given. Further we give a short review of basic Field Theory. After discussing on Ruler and Compass Constructions and Splitting Fields, we come to the Foundations of Galois Theory, which is the body of Chapter 2. We present the *Galois correspondence* and *Fundamental Theorem of Galois Theory*. In the last section of this chapter we prove *The Galois Criterion for Solvability by Radicals*. This is a criterion that is used to determine which equations are solvable and which are insolvable by radicals.

Chapter 3 studies Cogalois Theory. In this chapter we follow the monograph [1] by T. Albu. Firstly, we present some basic facts which are needed in the sequel. Then we prove *The Vahlen-Capelli Criterion* which is a criterion to decide when the binomials $X^n - a$ are irreducible over an arbitrary field. Then we introduce some concepts which play an important role in Cogalois Theory. These are the concepts of *G-radical* and *G-Kneser extension*. Roughly speaking, a radical extension is a field extension E/F such that E is obtained by adjoining to F an arbitrary set of “radicals” over F , that is, of elements of $x \in E$ such that $x^n = a$ for some $n \in \mathbb{N}^*$. We can denote x by $\sqrt[n]{a}$ and call it an n -th radical of a . So, if E/F is a radical extension, then we have $E = F(R)$, where R is a set of radicals over F . But we can replace R by the subgroup $F^* \subseteq G = F^* \langle R \rangle$ of the multiplicative group E^* of E generated by F^* and R . So, we have $E = F(G)$, where G containing F^* , is a subgroup of E^* . These extensions are called *G-radical extensions*. Note that this concept is different from the one used in Galois Theory, but coincides for simple extensions. A finite extension E/F is defined as *G-Kneser*, when it is *G-radical* and has the following property, $[G/F^*] = [E : F]$. Then we prove *The Kneser Criterion* which characterizes finite separable *G-Kneser* extensions.

In 3.3, we study Cogalois extensions. In this section we provide the definition of a Cogalois extension. A *Cogalois extension* is a field extension E/F which is $T(E/F)$ -Kneser. $T(E/F)$ is the subgroup of the multiplicative group E^* of E , such that the

factor group $T(E/F)/F^*$ is the torsion group of the factor E^*/F^* ($T(E/F)$ is the set of all elements of E^*/F^* which have finite order). The group $T(E/F)/F^*$ is called the *Cogalois group* of the extension E/F .

The *Greither-Harrison Criterion* that characterizes Cogalois extensions is also given in this chapter. Some examples and computations of Cogalois Group of a given field extension are also presented. Also the Cogalois groups of quadratic extensions of \mathbb{Q} are computed. Then we define the strongly G -Kneser extensions. Before defining this concept, we present a general discussion on the dual concepts, Galois connections and Cogalois connections. To any G -radical extension E/F , finite or infinite, a canonical *Cogalois connection* :

$$\xi \begin{array}{c} \xrightarrow{\varphi} \\ \xleftarrow{\psi} \end{array} \mathcal{G}$$

where

$$\varphi : \xi \longrightarrow \mathcal{G}, \varphi(K) = K \cap G,$$

$$\psi : \mathcal{G} \longrightarrow \xi, \psi(H) = F(H),$$

ξ is the lattice Intermediate(E/F) of all subfields of E containing F , and \mathcal{G} is the lattice $\{H \mid F^* \leq H \leq G\}$, is associated.

A *strongly G -Kneser extension* is a finite G -radical extension such that any subfield of K of E , containing F , the extension K/F is $K^* \cap G$ -Kneser. These extensions are precisely the G -Kneser extensions for which the maps

$$\alpha : \underline{\text{Intermediate}}(E/F) \longrightarrow \underline{\text{Subgroups}}(G/F^*), \alpha(K) = (K \cap G)/F^*,$$

and

$$\beta : \underline{\text{Subgroups}}(G/F^* \longrightarrow \underline{\text{Intermediate}}(E/F), \beta(H/F^*) = F(H)$$

are isomorphisms of lattices, inverse to one another. So, a strongly G -Kneser extension E/F is also defined as a G -Kneser extension with G/F^* -Cogalois correspondence.

In the following section, a special name to the separable field extensions E/F with G/F^* -Cogalois correspondence is given. They are called *G -Cogalois extensions*.

These extensions are characterized within the class of G -Kneser extensions by means of n -*Purity Criterion*, where n is the exponent of the quotient group G/F^* , which is finite. These extensions in Cogalois Theory play the same role as those of Galois extensions in Galois Theory. That's why they are so important in Cogalois Theory. Lastly, we are going to present some examples of G -Cogalois extensions.



Chapter 1

PRELIMINARIES

General Notation. In this chapter we present some general notation and terminology that are used throughout the Thesis.

Numbers and Sets

$\mathbb{N} = \{0, 1, 2, \dots\} =$ the set of all natural numbers

$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$

$\mathbb{Z} =$ the set of all rational integers

$\mathbb{Q} =$ the set of all rational numbers

$\mathbb{R} =$ the set of all real numbers

$\mathbb{C} =$ the set of all complex numbers

$S^* = S \setminus \{0\}$ for any $\emptyset \neq S \subseteq \mathbb{C}$

$S_+ = \{x \in S \mid x \geq 0\}$ for any $S \subseteq \mathbb{R}$

$S_+^* = \{x \in S \mid x > 0\}$ for any $S \subseteq \mathbb{R}$

$m \mid n$ m divides n

$\gcd(m, n) =$ the greatest common divisor of m and n

$\text{lcm}(m, n) =$ the least common multiple of m and n

$\varphi(n) =$ the Euler function of n

$\mathbb{P} = \{p \in \mathbb{N}^* \mid p \text{ prime}\}$

$\mathcal{P} = (\mathbb{P} \setminus \{2\}) \cup \{4\}$

$$\mathbb{P}_n = \{p \mid p \in \mathbb{P}, p \mid n\} \text{ for any } n \in \mathbb{N}$$

$$\mathbb{D}_n = \{m \mid m \in \mathbb{N}, m \mid n\} \text{ for any } n \in \mathbb{N}$$

$$\mathcal{P}_n = \mathcal{P} \cap \mathbb{D}_n \text{ for any } n \in \mathbb{N}$$

$$|M| = \text{the cardinality of an arbitrary set } M$$

$$1_M = \text{the identity map on the set } M$$

$$f|_A = \text{the restriction of a map } f : X \longrightarrow Y \text{ to } A \subseteq X$$



Groups

Unless otherwise stated G denotes throughout this Thesis a multiplicative group with identity element e .

1	the group with only one element
$H \subseteq G$	H is a subset of G
$H \leq G$	H is a subgroup of G
$x \equiv y \pmod{H}$	$x^{-1}y \in H$
$H \triangleleft G$	H is a normal subgroup of G
$H \vee K$	= the subgroup generated by $H \cup K$
$\bigvee_{i \in I}$	= the subgroup generated by $\bigcup_{i \in I} H_i$
S^n	= $\{x^n \mid x \in S\}$ for any $\emptyset \neq S \subseteq G$ and $n \in \mathbb{N}$
<u>Subgroups</u> (G)	= the lattice of all subgroups of G
$\langle M \rangle$	= the subgroup of G generated by the subset $M \subseteq G$
$\langle g_1, g_2, \dots, g_n \rangle$	= the subgroup of G generated by the subset $\{g_1, g_2, \dots, g_n\} \subseteq G$
$(G : H)$	= the index of the subgroup H in G
xH	= the left coset $\{xh \mid h \in H\}$ of $x \in G$ modulo $H \leq G$
G/H	= the quotient group of the group G modulo H where $H \triangleleft G$
\mathbb{Z}_n	= the quotient group $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n
S_n	= the symmetric group of degree n
A_n	= the alternating group of degree n
$\text{ord}_G(g)$	= $\text{ord}(g)$ = the order of an element $g \in G$
$t(G)$	= the set of all elements of G having finite order, i.e., the torsion group of the group G .

$t_p(G)$ = the set of all elements of G having order a power
of a prime number p

$$\prod_{i \in I} G_i = \{(x_i)_{i \in I} \mid x_i \in G_i, \text{ for all } i \in I\}$$

the (external) direct product of an arbitrary family $(G_i)_{i \in I}$ of groups

$$\bigoplus_{i \in I} G_i = \{(x_i)_{i \in I} \in \prod_{i \in I} G_i \mid x_i = e_i \text{ for all but finitely many } i \in I\}$$

the (external) direct sum of an arbitrary family $(G_i)_{i \in I}$ of groups

$$\bigoplus_{i \in I} H_i = \bigvee_{i \in I} H_i = \text{the internal direct sum of an independent family}$$

$(H_i)_{i \in I}$ of normal subgroups of G



Rings

All rings given in this Thesis have unit elements.

$$A^* = A \setminus \{0\} \text{ for any subset } A \text{ of a ring } R$$

$$U(R) = \text{the group of all units of a ring } R$$

$$\mathbb{F}_q = \text{the finite field of } q \text{ elements}$$

$$(x_1, x_2, \dots, x_n) = \left\{ \sum_{1 \leq i \leq n} r_i x_i \mid r_1, r_2, \dots, r_n \in R \right\} = \text{the left ideal of } R \\ \text{generated by } x_1, x_2, \dots, x_n \in R$$

$$(x) = Rx = \text{the principal left ideal of } R \\ \text{generated by } x \in R$$

$$R[X_1, \dots, X_n] = \text{the polynomial ring in the indeterminates} \\ X_1, \dots, X_n \text{ with coefficients in the ring } R$$

$$\deg(f) = \text{the degree of a polynomial } f \in R[X]$$

$$Q(R) = \text{the field of quotients of the domain } R$$

$$F(X_1, \dots, X_n) = Q(F[X_1, \dots, X_n]) = \text{the field of rational} \\ \text{fractions in the indeterminates } X_1, \dots, X_n \\ \text{with coefficients in the field } F$$

$$\mu_n(F) = \{x \in F \mid x^n = 1\}, F \text{ a field, } n \in \mathbb{N}^*$$

$$F^n = \{x^n \mid x \in F\}, F \text{ a field, } n \in \mathbb{N}^*$$

Chapter 2

GALOIS THEORY

Before listing the important concepts that are used throughout this Thesis, we briefly mention about Galois' life.

2.1 *The Life of Galois*

Évariste Galois was born on October 25, 1811 in Bourg-la-Reine, France. His father was Nicholas-Gabriel Galois, and his mother was Adelaide-Marie Demante. They were both well educated in the subjects of philosophy, classical literature and religion. In his childhood, Évariste's mother helped him to be good at Greek and Latin. He was also influenced by her skepticism toward religion.

His father was a republican. He was the head of the village liberal party, but in 1814 when Louis XVIII returned to the throne, he became the mayor of the town. Galois's mother was the daughter of the jurisconsult. It can be correctly said that Galois was influenced by his parents' liberal ideas. On October 6, 1823 Galois entered a preparatory school, named College de Louis-le Grand which still continues education in Paris. That school was a place where he had the chance to express his political ideas. In Galois' first term in that school, the students rebelled and refused to sing in the chapel. Then, forty students, whom were believed to lead the insurrection, were expelled. It was not known whether Galois was among the ones who were expelled or not. But there is no harm in saying that these events had made an impression on him.

In the first two years of school, Galois was successful. He received the first prize in Latin and he had some other remarkable successes. But then everything started to become worse. Galois was asked to repeat his third year. In those hard times Galois

found a safe place to hide. He took a serious interest in mathematics. He discovered Legendre's text on geometry, and soon he had read Lagrange's original memoirs: *Resolution of Numerical Equations Theory of Analytic Functions and Lessons on the Calculus of Functions*. Without a doubt, his ideas on the theory of equations originated in Lagrange. Since he discovered the hidden secrets of mathematics, he neglected other courses. Some of his teachers were unimpressed by his attitude, and they thought that he was dissipated.

His mathematics teacher, M. Vernier, recommended him to work systematically. But Galois did not take his advise and without being well-prepared, he took the examination to "l'École Polytechnique" a year early. But he was rejected.

In 1828, Galois enrolled in an advance mathematics course given by Louis-Paul-Émile Richard who noticed his ability in mathematics. He thought that Galois should be admitted to the Polytechnique without examination, since he believed that his high talent would not let him to be successful in an examination which would be prepared with poor examination techniques.

The next year Galois published his first research paper *Proof of a Theorem on Periodic Continued Fractions* in *Annales de Gergonne*. At the same time he was working on the theory of polynomial equations. At the age of 17, he submitted his first researches on the solubility of equations of prime degree to the Academy of Sciences. At that time, Augustin-Louis Cauchy was the referee. In Rothman's notes, there was a belief that Cauchy lost the manuscript or he got rid of it deliberately. But on the other hand, René Taton (1971) has discovered a letter, which proved that he did not lose Galois's memoirs but had planned to present them to the Academy in January 1830, of Cauchy in the archives of the Academy. But on 25 of January Cauchy did not present Galois's paper.

Taton suggested that Cauchy found Galois's ideas remarkable and advised Galois to prepare a new version for the Grand Prize in Mathematics. But we are not sure whether this is the exact truth or not. What we know for sure is that Galois made such a submission to the competition. Although Cauchy had conferred the highest

price on Galois about his works on numerical equations, the memoir is lost in a strange way and the prize is given without participation of Galois.

The same year, on the second of July, 1829, Galois's father committed suicide. The priest of Bourg-la-Reine had signed Mayor Galois's name to a number of maliciously forged epigrams directed at Galois's own relatives. But M. Galois could not get over such an attack. Galois was deeply effected by this event and the years after his father's death were very difficult for him. A few days later Galois failed the entrance examination to l'École Polytechnique for the second and the last time.

Since Galois was planning to continue his education in l'École Polytechnique and it did not require the Bachelor examinations, he did not study for his final examinations. But now that he had failed to be admitted to l'École Polytechnique, he decided to enter l'École Normale which was less prestigious than the Polytechnique at that time. He prepared himself for his final examinations and he did well in mathematics and science. In literature he was not much good, but he obtained both Bachelor of Science and Bachelor of Letters on 29 December 1829.

In February 1830, Galois presented a new version of his research to the Academy of Sciences for the competition of Grand Prize in Mathematics. His paper reached the secretary, Joseph Fourier, and he took it home to read. However he died before reading it, and Galois' entry could not be found among his papers. But it may not have been Fourier who lost the entry, since among Grand Prize committee, there were also Legendre, Sylvestre-François Lacroix, and Louis Poinsot. On the other hand, in Galois's eyes the repeated loss of his papers could not be an accident. As he said "The loss of my memoir is a very simple matter, and it was with M. Fourier, who was supposed to have read it and, at the death of this savant, the memoir was lost." In April, in spite of the things happened in February, Galois published a paper, *An analysis of a Memoir on the Algebraic Resolution of Equations* and in June, he published *Notes on the Resolution of Numerical Equations* and the article *On the Theory of Numbers*, which were very important.

During the July revolution of 1830, the Director of l'Ecole Normale, M. Guigniault,

locked the students in, so that they would not be able to fight on the streets. Galois tried to escape but he failed and missed the revolution. In December of that year, M. Guigniault was engaging in polemics against students in lots of newspapers. Then, Galois wrote a blistering letter to the *Gazette des Écoles*.

Galois was expelled because of that letter. This happened on January 4, but Galois left the school immediately and joined the Artillery of the National Guard, a branch of the militia which was composed of mostly republicans. On 21 December 1830, the Artillery of the National Guard, in which Galois was serving, was stationed near the Louvre and were waiting for the verdict of the trial of four ex-ministers. The decision would be to execute or to give them life sentences. If they received only life sentences, the Artillery was planning to rebel. Before the verdict was announced, the Louvre was surrounded by the full National Guard and by other troops. Then the verdict was announced and the ministers had been given imprisonment. But it did not erupt in fighting. On 31 December, the Artillery of the National Guard was abolished by the king because they were thought of as a threat to the throne.

In January 1831, Galois was no longer a student and he knew that he had to do something in order to make a living. Then he decided to give private lessons on Advanced Algebra. Forty students enrolled, but his attempt to give lessons did not continue for long because he was too involved in politics.

On 17 January he submitted a third version of his memoir to the Academy: *On the Conditions of Solvability of Equations by Radicals*. Siméon Poisson and Lacroix were the appointed referees. But he did not receive any answer from them in two months. So, he decided to write a letter in order to learn the reason of it. But he received no reply.

During the spring of 1831, Galois' behavior became more extreme. In the ninth of May, 1831, about two hundred young republicans held a banquet to protest against the royal order disbanding the artillery which Galois had joined. Toasts were given to the Revolutions of 1789 and 1793 and to the Revolution of 1830. Galois was seen with his glass in one hand, and his open pocket knife in the other. His companions

interpreted this as a threat against the life of the King.

The next day Galois was arrested and thrown into the prison at Sainte-Pelagie. Probably because of his youth, he was freed on 15 June.

On 4 July, he received a letter about his memoir. Poisson declared it “incomprehensible”. According to the referees, Galois’ entry did not yield any workable criterion to determine whether an equation is solvable by radicals. Tignol says “the Galois Theory did not correspond to what was expected, it was too novel to be readily accepted”.

On 14 July, Galois and one of his friends were leading a Republican Demonstration. Galois was wearing the uniform of the Artillery and carrying a knife and a loaded rifle. Since it was illegal to wear the uniform and to be armed, they were arrested. He stayed in prison nearly six months and he worked on mathematics there. Because of cholera epidemic he was transferred to a hospital. Soon he was set free. In the first times of his freedom, he experienced his first and only love affair. The lady’s name was believed to be Stéphanie-Felicie Poterin du Motel. But he was rejected and it was hard for him to get over it.

Soon Galois was challenged to a duel, seemingly because of his advances toward this lady. But the circumstances are mysterious. One thought assets that Galois’ interest in Mlle. du Motel was used by his political opponents. The other thought assets that Galois was assassinated by a police spy. But Alexandra Dumas says that Galois was killed by a republican, Pescheux D’Herbinville and it was clear that he was not a police spy. So, the duel was exactly what it appeared to be. Galois’ own word also supports this matter:

“I beg patriots and my friends not to reproach me for dying otherwise than for my country. I die the victim of an infamous coquette and her two dupes. It is in a miserable piece of slander that I end my life. Oh! Why die for something so little, so contemptible?... Forgive those who kill me for they are of good faith.”

On 29 May, the eve of the duel Galois wrote down his discoveries in a letter in order to be sent to his friend Auguste Chevalier. This letter was later published in *Revue Encyclopédique*. In that letter Galois made the connection between the groups

and polynomial equations, and stated that an equation is solvable by radicals if its group is solvable. He also mentioned many other ideas in his letter, about elliptic functions and the integration of algebraic functions. His letter was actually for the posterity. After his death, his few supporters managed to get the letter to Joseph Liouville who edited his work and published them with this letter to Chevalier. With the help of this book Galois gained the appreciation that he had always deserved. His letter to Chevalier ended with these words:

“Ask Jacobi or Gauss publicly to give their opinion, not as to the truth, but as the importance of these theorems. Later there will be, I hope, some people who will find it to their advantage to decipher all this mess..”

It was not until Liouville republished Galois’s original work in 1846 that its significance was noticed at all. Serret, Bertrand and Hermite had listened Liouville’s lectures on Galois theory and had begun to contribute to the subject but it was C. Jordan who was the first to formulate the direction the subject would take.

Galois’ discoveries enabled him to prove the problem, *why the equations higher than the fourth degree could not generally be solved by radicals*. His success mostly comes from his approach which is directed toward the algebraic structure of the problem. He felt that he could solve this problem which uses field theory, by reducing it into a group theoretical one. Then, not only his idea lead him to the right solution, but also it gave birth to modern algebra.

2.2 Some Results on Solvable Groups

In this section we present some basic facts on solvable groups that will be frequently used in the sequel.

Definition 2.2.1. *A normal series of a group G is a chain of subgroups*

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_n = G,$$

where $G_i \triangleleft G_{i+1}$ for all $i \in \{0, 1, 2, \dots, n-1\}$. The quotient groups G_{i+1}/G_i , where $i \in \{0, 1, 2, \dots, n-1\}$ are called the factors of the normal series. \square

Definition 2.2.2. A group G is said to be solvable if it has a normal series whose factors are Abelian. \square

Now we list some important results on solvable groups.

Proposition 2.2.3. Let G be a finite group. Then G is solvable if and only if G has a normal series whose factors are cyclic groups of prime order. \square

Proposition 2.2.4. Any subgroup and any homomorphic image of a solvable group is solvable. In particular, any quotient group of a solvable group is solvable. \square

Proposition 2.2.5. Let $N \triangleleft G$. If N and G/N are solvable then G is also solvable. \square

Examples 2.2.6. (1) Any Abelian group G is solvable since $1 \triangleleft G$ is a normal series with Abelian factor $G/1$.

(2) Consider the group S_3 . We know that $1 \triangleleft A_3 \triangleleft S_3$, and the factors of this normal series are $S_3/A_3 \cong \mathbb{Z}_2$ and $A_3/1 \cong \mathbb{Z}_3$. Hence, these factors are cyclic, so Abelian. Therefore S_3 is solvable.

More generally, S_n is solvable if and only if $1 \leq n \leq 4$. By (1), S_1 and S_2 are solvable since they are Abelian and by (2), S_3 is solvable. Now we show that S_4 is solvable. We claim that

$$1 \triangleleft K \triangleleft A_4 \triangleleft S_4$$

is a normal series of S_4 , where

$$K = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

We are going to show that $K \triangleleft A_4$. The left cosets of K in A_4 are $K, (1,2,3)K, (2,3,4)K$, and the right cosets K in A_4 are $K, K(1,2,3), K(2,3,4)$. But $K(1,2,3) = (1,2,3)K$, and also $K(2,3,4) = (2,3,4)K$. So, every right coset of K in A_4 is a left coset of K in A_4 . Hence, $K \triangleleft A_4$. Since $|A_4/K| = 12/4 = 3$, we have $A_4/K \cong \mathbb{Z}_3$, so A_4/K is Abelian. We have also $S_4/A_4 \cong \mathbb{Z}_2$ and $K/1 \cong K$ and K is isomorphic to the Klein-4 group, which is Abelian. Thus,

$$1 \triangleleft K \triangleleft A_4 \triangleleft S_4$$

is a normal series of S_4 with Abelian factors. Therefore, S_4 is solvable.

Conversely assume that S_n is solvable for $n \geq 5$. Then by Proposition 2.2.4, A_n would be solvable since $A_n \leq S_n$, for all $n \in \mathbb{N}^*$. But we know that A_n is simple for $n \geq 5$. So,

$$1 \triangleleft A_n$$

is the only normal series of A_n , for $n \geq 5$. Since $A_n/1 \cong A_n$ is clearly non-Abelian, for $n \geq 5$, this leads to a contradiction. Thus, we have shown that S_n is solvable if and only if $1 \leq n \leq 4$. \square

2.3 Basic Field Theory

In this section we present the basic terminology, notation and results in Field Theory which are used throughout the Thesis. Firstly, we recall the definition of a field.

Definition 2.3.1. A field F is a commutative unital ring with $1 \neq 0$, in which every nonzero element is invertible. \square

Now we define the characteristic of a field.

Definition 2.3.2. The characteristic of a field F is a natural number defined by:

$$\text{Char}(F) = \begin{cases} n & \text{if } n \in \mathbb{N} \\ 0 & \text{if } n = \infty \end{cases}$$

where $n \in \mathbb{N}^* \cup \{\infty\}$ is the order of the identity element 1 in the Abelian group $(F, +)$ of the field F . If $\text{Char}(F) \neq 0$ then it is necessarily a prime number. \square

Definition 2.3.3. The characteristic exponent $e(F)$ of a field F is defined by

$$e(F) = \begin{cases} 1 & \text{if } \text{Char}(F) = 0 \\ p & \text{if } \text{Char}(F) = p > 0 \end{cases}$$

A field F is said to be perfect if $F = F^{e(F)}$. \square

Field Extension

Definition 2.3.4. Let $F \subseteq E$ be fields. If F contains the identity element of E , and if it is closed under subtraction, multiplication, and inverses, then we say that F is a subfield of E .

If F is a subfield of the field E , then E is said to be an overfield (extension field) of F . We call the pair (F, E) a field extension, where F is a subfield of E (or E is an overfield of F), in this case, we write E/F . Any subfield K of E with $F \subseteq K$ is called an intermediate field of the extension E/F . A subextension (resp. quotient extension) of the extension E/F is any extension of the form K/F (resp. E/K), where K is an intermediate field of the extension E/F . \square

If E/F is a field extension then we can consider E as a vector space over F . We call the dimension of this vector space, the degree of E over F and write it as $[E : F]$. If $[E : F] < \infty$, then we say that E/F is a finite extension.

An extension is called *quadratic* (resp. *cubic*, *quartic*, *quintic*) if $[E : F] = 2$ (resp. $[E : F] = 3$, $[E : F] = 4$, $[E : F] = 5$).

Proposition 2.3.5. Let F, K, E be fields with $F \subseteq K \subseteq E$. Then $[E : F]$ is finite if and only if $[E : K]$ and $[K : F]$ are finite, and in this case $[E : F] = [E : K] \cdot [K : F]$ holds.

Proof. Suppose that $[E : F]$ is finite. Since K is a subspace of E containing F , $[K : F]$ is finite. $[E : K]$ is also finite since a basis for E over F spans E over K .

Conversely, suppose that $[K : F] = m < \infty$ and $[E : K] = n < \infty$. Let $\{u_1, \dots, u_m\}$ be a basis for K/F and let $\{v_1, \dots, v_n\}$ be a basis for E/K . We claim that

$$\{u_j v_i \mid 1 \leq j \leq m, 1 \leq i \leq n\}$$

is a basis for E/F . If we can show that, then we deduce that $[E : F]$ is finite and equals to nm . In order to show that

$$\{u_j v_i \mid 1 \leq j \leq m, 1 \leq i \leq n\}$$

forms a basis for E/F , we must first show that this set spans E and it is linearly independent over F . Let x be an element of E . We can write

$$x = \sum_{i=1}^n a_i v_i$$

where $a_i \in K$ for each $1 \leq i \leq n$. Since $\{u_1, \dots, u_m\}$ is a basis for K/F , each a_i can be written as $a_i = \sum_{1 \leq j \leq m} c_{ij} u_j$ with $c_{ij} \in F$. And then this gives

$$x = \sum_{i,j} c_{ij} u_j v_i.$$

Hence, $\{u_j v_i \mid 1 \leq j \leq m, 1 \leq i \leq n\}$ spans E/F . We are going to show that this set is linearly independent. Suppose that

$$\sum_{i,j} c_{ij} u_j v_i = 0$$

where each $c_{ij} \in F$. We have to show that $c_{ij} = 0$ for each i, j . We can write the above equality as

$$0 = \sum_{1 \leq i \leq n} \left(\sum_{1 \leq j \leq m} c_{ij} u_j \right) v_i.$$

We know that $\sum_{1 \leq j \leq m} c_{ij} u_j \in K$, and this gives that $\sum_j c_{ij} u_j = 0$ for all i , since $\{v_1, \dots, v_n\}$ is a basis for E/K . Since $c_{ij} \in F$ for each i, j and $\{u_1, \dots, u_m\}$ is a basis for K/F we obtain $c_{ij} = 0$ for all j . Hence, $\{u_j v_i \mid 1 \leq j \leq m, 1 \leq i \leq n\}$ is a basis for E/F . Therefore, $[E : F]$ is finite and

$$[E : F] = nm = [E : K] \cdot [K : F],$$

as desired. □

F-homomorphism, F-isomorphism, Galois group

If E/F and L/F are two extensions, then an F -homomorphism from the field E into the field L is any ring homomorphism $\sigma : E \rightarrow L$ that fixes F pointwise, i.e. $\sigma(a) = a$, for all $a \in F$. Any F -homomorphism of fields is necessarily an injective map. An F -isomorphism is a surjective (hence bijective) F -homomorphism. An F -automorphism

of E is any F -isomorphism from E into itself. The set of all F -automorphisms of E is a group under the binary operation of composition, called the Galois group of the extension E/F , and denoted by $\text{Gal}(E/F)$.

Poset, Lattice, Isomorphism, Anti-isomorphism

A *partially ordered set*, or *poset*, is a pair (P, \leq) consisting of a nonempty set P and a binary relation \leq on P which is reflexive, anti-symmetric, and transitive. A poset is also denoted by \dot{P} . The opposite poset of P is denoted by P^{op} .

If every two elements x, y in a poset L have a least upper bound, $x \vee y$ (also denoted by $\text{sup}(x, y)$) and a greatest lower bound $x \wedge y$ (also denoted by $\text{inf}(x, y)$), then L is said to be a lattice. A *complete lattice* is a poset in which every subset A has a least upper bound $\bigvee_{x \in A} x$ (also denoted by $\text{sup}(A)$) and a greatest lower bound $\bigwedge_{x \in A} x$ (also denoted by $\text{inf}(A)$).

A *poset homomorphism* (resp. a *poset anti-homomorphism*) from a poset P into a poset P' is a map $f : P \rightarrow P'$ which is *increasing*, or *order-preserving* (resp. *decreasing*, or *order-reversing*), that is, satisfies the following condition:

$$\forall x \leq y \text{ in } P \implies f(x) \leq f(y)$$

$$\text{(resp. } \forall x \leq y \text{ in } P \implies f(y) \leq f(x)\text{)}.$$

A *poset isomorphism* (resp. a *poset anti-isomorphism*) from a poset P into a poset P' is a bijective poset homomorphism (resp. poset anti-homomorphism) $f : P \rightarrow P'$ such that its inverse $f^{-1} : P' \rightarrow P$ is a poset homomorphism (resp. poset anti-homomorphism).

If L and L' are two lattices, then a *lattice homomorphism* resp. (*lattice anti-homomorphism*) from L into L' is a map $f : L \rightarrow L'$ satisfying the following conditions:

$$f(x \wedge y) = f(x) \wedge f(y) \text{ and } f(x \vee y) = f(x) \vee f(y), \forall x, y \in L$$

(resp. $f(x \wedge y) = f(x) \vee f(y)$ and $f(x \vee y) = f(x) \wedge f(y)$, $\forall x, y \in L$).

Any lattice isomorphism between complete lattices commutes with arbitrary meets and joins.

A bijection $f : L \rightarrow L'$ between two lattices L and L' is a *lattice isomorphism* (resp. *lattice anti-isomorphism*) if and only if f and its inverse f^{-1} are both order-preserving (resp. order-reversing) maps, i.e. if and only if f is a poset isomorphism (resp. poset anti-isomorphism).

Lattice of Subextensions

By Subextensions(E/F) we will denote the set of all subextensions of E/F . Note that Subextensions(E/F) is a poset, that is, a partially ordered set, with respect to the partial order \leq defined as follows:

$$K/F \leq L/F \iff K \text{ is a subfield of } L.$$

Actually, this poset is a complete lattice, where

$$\inf_{i \in I} (K_i/F) = \left(\bigcap_{i \in I} K_i \right) / F,$$

$$\sup_{i \in I} (K_i/F) = F \left(\bigcup_{i \in I} K_i \right) / F,$$

and $F(\bigcup_{i \in I} K_i)$ is the subfield of E obtained by adjoining the set $\bigcup_{i \in I} K_i$ to the field F (see Adjunction).

Note that the lattice Subextensions(E/F) is essentially the same with the lattice Intermediate(E/F) of all intermediate fields of the extension E/F .

Tower of Fields

A finite chain

$$E_0 \subseteq E_1 \subseteq E_2 \subseteq \dots \subseteq E_n$$

of fields, where $n \geq 2$ and E_i is a subfield of E_{i+1} , for every $i = 0, \dots, n-1$ is called a *tower of fields*.

*Adjunction**Ring Adjunction*

Let E be a ring, and let R be a subring of E . If A is any subset of E , then $R[A]$ denotes the smallest subring of E containing both R and A as subsets. We have

$$R[A] := \bigcap_{T \in S_A} T$$

where $S_A = \{T \mid A \cup R \subseteq T, T \text{ is a subring of } E\}$. Clearly, $R[A]$ is a subring of E , and it is called the subring of E obtained by adjoining to R the set A . We call the procedure of obtaining $R[A]$ from a subring R of E and a subset A of E a *ring adjunction*.

Now we describe the elements of $R[A]$. Clearly, $R[\emptyset] = R$. Let $A = \{a_1, a_2, \dots, a_n\}$ be a nonempty, finite subset of E . Then we denote $R[\{a_1, a_2, \dots, a_n\}] = R[a_1, a_2, \dots, a_n]$. We claim that

$$R[a_1, a_2, \dots, a_n] = \{f(a_1, a_2, \dots, a_n) \mid f \in R[X_1, \dots, X_n]\},$$

where $f(a_1, a_2, \dots, a_n)$ is the “value” in (a_1, a_2, \dots, a_n) of the polynomial f .

First observe that

$$R[A \cup B] = R[A][B] = R[B][A],$$

where A and B are subsets of E . By the definition of ring adjunction, $R[A][B]$ is the subring of E obtained by adjoining B to the subring $R[A]$ of E . We claim that $R[A][B]$ coincides with the subring $R[A \cup B]$, which is the subring of E obtained by adjoining $A \cup B$ to R . Firstly, $R[A \cup B]$ contains $R[A]$ and B since $R[A] \subseteq R[A \cup B]$, and $B \subseteq R[A \cup B]$. By the definition of ring adjunction, the subring of E which is obtained by adjoining to $R[A]$ the set B , that is $R[A][B]$, lies in $R[A \cup B]$. Hence, $R[A][B] \subseteq R[A \cup B]$. Now we are going to show the other inclusion. It is clear that $R, A \cup B \subseteq R[A \cup B]$. So, by the same reasoning, we obtain $R[A \cup B] \subseteq R[A][B]$. Hence, $R[A \cup B] = R[A][B]$. If we repeat the argument by adjoining A to the subring $R[B]$, we obtain $R[A \cup B] = R[B][A]$, and we are done.

Let $A = \{a_1, a_2, \dots, a_n\}$. If we do induction on n , then we can generalize the above result. So, we obtain

$$R[a_1, a_2, \dots, a_n] = (((R[a_1])[a_2]) \dots [a_{n-1}])[a_n], \quad (2.3.1)$$

that is, $R[a_1, a_2, \dots, a_n]$ is obtained by adjoining single elements to the previously constructed subrings. According to this result, in order to describe the elements of $R[A]$, we can start by studying subrings of the form $R[a]$. We can see that the elements of $R[a]$ are of the form

$$b_0 + b_1a + b_2a^2 + \dots + b_na^n,$$

with $n \in \mathbb{N}$ arbitrary and $b_i \in R$ for all i , $0 \leq i \leq n$. These are just the polynomial expressions in a with coefficients in R . Clearly, $R[a]$ contains all such elements. We can also show that the set of polynomial expressions in a with coefficients from R form a subring of R . By definition of ring adjunction, we can easily see that this subring coincides with $R[a]$.

Now, using the above result and Equation (2.3.1), we deduce that

$$R[a_1, a_2, \dots, a_n] = \{f(a_1, a_2, \dots, a_n) \mid f \in R[X_1, \dots, X_n]\}.$$

Now if A is any subset of E , then we can show that

$$R[A] = \bigcup_{C \in \mathcal{F}_A} R[C],$$

where \mathcal{F}_A denotes the set of all finite subsets of A . Each subring $R[C]$ of E is contained in $R[A]$, where $C \in \mathcal{F}_A$; hence, $\bigcup_{C \in \mathcal{F}_A} R[C] \subseteq R[A]$. Clearly, this union contains R and A . So if it is a subring of E , then it must be equal to $R[A]$, since $R[A]$ is the smallest subring of E containing R and A . To show that this union is a subring of E , let $\alpha, \beta \in \bigcup_{C \in \mathcal{F}_A} R[C]$. Then there are some finite subsets C, D of A such that $\alpha \in R[C]$ and $\beta \in R[D]$. Then both α, β belong to $R[C \cup D]$. So, clearly, $\alpha \pm \beta, \alpha\beta$ all lie in $\bigcup_{C \in \mathcal{F}_A} R[C]$. So, this union is a subring of E . Hence,

$$R[A] = \bigcup_{C \in \mathcal{F}_A} R[C].$$

Field Adjunction

Let E/F be a field extension, and let A be a subset of E . $F(A)$ denotes the smallest subfield of E containing both F and A as subsets, i.e.,

$$F(A) := \bigcap_{K \in \mathcal{T}_A} K,$$

where $\mathcal{T}_A = \{K \mid A \cup F \subseteq K, K \text{ is a subfield of } E\}$.

$F(A)$ is called the subfield of E that is *obtained by adjoining A to the field F* and the extension $F(A)/F$ is the *subextension* of E/F generated by the set A . We call the procedure of obtaining the subfield $F(A)$ from a field F and a subset A of E a *field adjunction*.

As in the ring case, we have

$$F(A) = \bigcup_{S \in \mathcal{F}_A} F(S). \quad (2.3.2)$$

We denote by \mathcal{F}_A the set of all finite subsets of A . As in the ring case again, we have $F(A \cup B) = F(A)(B) = F(B)(A)$ where A, B are subsets of E .

For any field extension E/F and any subset A of E , we claim that $F(A)$ is the field of quotients of the integral domain $F[A]$. Firstly, take $A = \{a\}$. Since $F[a]$ is a subring of the field E , it is an integral domain. So, all possible quotients of the elements of $F[a]$ belong to E . Then we have

$$F \cup \{a\} \subseteq F[a] \subseteq Q(F[a]) \subseteq E.$$

By the definition of $F(a)$, we obtain $F(a) \subseteq Q(F[a])$.

$F(a)$ is a subring of E containing both F and a . So, $F[a] \subseteq F(a)$. But $F(a)$ is a field, so it has to contain all possible quotients of the elements of $F[a]$. Thus, $Q(F[a]) \subseteq F(a)$. Therefore, $Q(F[a]) = F(a)$. If we take A to be any finite subset of E , then doing induction on the number of elements in A , we obtain the same result. Now if we take A to be an infinite subset of E , then by Equation (2.3.2), we have the same result. Hence, we have shown that $F(A)$ is the field of quotients of the integral domain $F[A]$, for any subset A of E .

Now we can list the elements of $F(A)$. Clearly, $F(\emptyset) = F$. For any nonempty finite subset $A = \{a_1, \dots, a_n\}$ of E , where E is an overfield of F ,

$$F(a_1, \dots, a_n) = \{f(a_1, \dots, a_n)(g(a_1, \dots, a_n))^{-1} \mid f, g \in F[X_1, \dots, X_n], g(a_1, \dots, a_n) \neq 0\}.$$

Finitely Generated Extension

A field extension E/F is said to be *finitely generated* (or of *finite type*) if $E = F(A)$ for some finite subset A of E . If $A = \{a_1, a_2, \dots, a_n\}$ then instead of $F(\{a_1, a_2, \dots, a_n\})$ we write $F(a_1, a_2, \dots, a_n)$.

Simple extension

An extension E/F is said to be *simple* if there exists $a \in E$, called a primitive element of E/F such that $E = F(a)$.

Compositum

Let E/F be a field extension and let $(K_i)_{i \in I}$ be a family of intermediate fields of the extension E/F . The *compositum* of $(K_i)_{i \in I}$ is the field $F(\bigcup_{i \in I} K_i)$ which is denoted by $\bigvee_{i \in I} K_i$. If the index set I is finite, then we denote the compositum of a family $(K_i)_{1 \leq i \leq n}$ also as $K_1 K_2 \dots K_n$.

The next result gives an upper bound for the degree of the compositum of two intermediate fields.

Proposition 2.3.6. *Let K and L and be two intermediate fields of the extension E/F .*

If $[K : F] = m$, $[L : F] = n$ and $[K \vee L : F] = t$ then $t < \infty$ if and only if both m and n are finite; in this case $m \mid t$ and $n \mid t$ and $t \leq mn$; if m and n are relatively prime then $t = mn$. \square

Algebraic Extension

Definition 2.3.7. Let E/F be a field extension, and let $u \in E$. We say that u is algebraic over F , if there exists $f \in F[X]$, $f \neq 0$ such that $f(u) = 0$. Otherwise we say that u is transcendental over F . \square

Let E/F be a field extension and $u \in E$. The evaluation map

$$\eta_u : F[X] \longrightarrow E,$$

which is defined as $\eta_u(f) = f(u)$, is a ring homomorphism. The image of this homomorphism is $F[u]$. Using the Fundamental Theorem of Isomorphism for Rings, we obtain

$$F[X]/\text{Ker}(\eta_u) \cong F[u].$$

Clearly,

$$u \text{ is transcendental over } F \iff \text{Ker}(\eta_u) = 0 \iff F[X] \cong F[u].$$

$$u \text{ is algebraic over } F \iff \text{Ker}(\eta_u) \neq 0.$$

We know that $\text{Ker}(\eta_u)$ is a principal ideal of $F[X]$, since $F[X]$ is a PID. So, if u is algebraic over F then the unique monic polynomial f which generates $\text{Ker}(\eta_u)$ is called the *minimal polynomial of u over F* . We denote it by $\text{Min}(u, F)$.

Proposition 2.3.8. Let E/F be a field extension, let $u \in E$ be algebraic over F , and let $f = \text{Min}(u, F)$ with $n = \text{deg}(f)$. Then

- (1) f is unique, irreducible in $F[X]$, and for all polynomials $g \in F[X]$ such that $g(u) = 0$ we have $f \mid g$.
- (2) $\{1, u, u^2, \dots, u^{n-1}\}$ is a basis of the vector space $F[u]$ over F , so $[F[u] : F] = n$.
- (3) $F[u]$ is a field, and in this case we have $F[u] = F(u)$.

Proof. We only prove part (3). Let $y \in F[u]$, $y \neq 0$ be arbitrary. Since $y \in F[u]$ we have $y = g(u) = a_0 + a_1u + a_2u^2 + \dots + a_mu^m$ where $a_i \in F$. Let $f = \text{Min}(u, F)$. Then by part (1), $f \in F[X]$, f is monic and irreducible, $f(u) = 0$ and $f \mid g$ for polynomials $g \in F[X]$ such that $g(u) = 0$. Let $\text{gcd}(f, g) = d$. Then $d \mid f$ and $d \mid g$. Since f is irreducible, we have either $d \sim 1$ or $d \sim f$ ¹. If $d \sim f$ then $f \mid g$, and this implies that $g = fh$ for some polynomial $h \in F[X]$. Then $y = g(u) = f(u)g(u) = 0$, which contradicts our assumption. So $d \sim 1$, which means that $\text{gcd}(f, g) \sim 1$. Then there exists $f_1, g_1 \in F[X]$ such that $1 = f \cdot f_1 + g \cdot g_1$.

Now evaluate this equation at u . Then $1 = f(u)f_1(u) + g(u)g_1(u)$. But, $f(u) = 0$. Then we have $1 = g(u)g_1(u)$. Since $g(u) = y$, we can take $g_1(u)$ as y^{-1} . Hence, all elements $y \in F[u]$, $y \neq 0$ are invertible, which means that $F[u]$ is a field. Therefore $F[u] = F(u)$. \square

Definition 2.3.9. Let E/F be an extension. We say that E/F is an algebraic extension, or E is algebraic over F , if every element of E is algebraic over F . Otherwise E/F is a transcendental extension or E is transcendental over F . \square

Proposition 2.3.10. An extension E/F is algebraic if and only if every subring A of E with $F \subseteq A$ is a field.

Proof. Let A be a subring of E with $F \subseteq A$. We have to show that for every $u \in A$, $u \neq 0$, $u^{-1} \in A$. Since $F \subseteq A$ and $u \in A$, $F[u] \subseteq A$. But since u is algebraic over F , part (3) of Proposition 2.3.8 says that $F[u]$ is a field. Hence, we have that $u \in F[u] \subseteq A \Rightarrow u^{-1} \in A$, and so A is a field.

Conversely, we show that u is algebraic over F , for every $u \in E$. If $u = 0$, then we are done. So, assume $u \neq 0$. We have $F \subseteq F[u] \subseteq E$, and $F[u]$ is a subring of E . Then, from our assumption $F[u]$ is a field. Since $u \in F[u]$ we have $u^{-1} \in F[u]$. So, there exists some $b_0, b_1, \dots, b_n \in F$, such that $u^{-1} = b_0 + b_1u + \dots + b_nu^n$. If we multiply both sides with u , then we obtain $1 = b_0u + b_1u^2 + \dots + b_nu^{n+1}$. So, we have obtained a nonzero polynomial $f = b_nX^{n+1} + b_{n-1}X^n + \dots + b_0X - 1 \in F[X]$. But u

¹ $a \sim b$ means that a and b are associate in divisibility.

is a root of this polynomial. Therefore, every element of E is algebraic over F , which means that E/F is an algebraic extension. \square

We list below some important properties of algebraic extensions.

- (1) The followings are equivalent for an extension E/F .
 - (a) E/F is a finite extension.
 - (b) E/F is algebraic and finitely generated.
 - (c) There exists finitely many algebraic elements u_1, u_2, \dots, u_n of E/F such that $E = F(u_1, u_2, \dots, u_n)$.
- (2) Let E/F be an extension, and let A be a subset of E consisting of algebraic elements over F . Then $F(A)/F$ is an algebraic extension, and so $F(A) = F[A]$.
- (3) Let $F \subseteq K \subseteq E$ be a tower of fields. Then E/F is an algebraic extension if and only if both E/K and K/F are algebraic extensions.

Splitting Field

Let F be a field and let $f \in F[X] \setminus F$. An overfield E of F is called a *splitting field over F* of f if the following conditions are satisfied.

- (1) f splits over E , that is, we have

$$f = c(X - r_1) \dots (X - r_n),$$

where $r_1, \dots, r_n \in E$ and $c \in F^*$.

- (2) There is no proper subfield E' of E which contains F such that f splits over E' , in other words $E = F(r_1, \dots, r_n)$. This means that E is minimal with the property (1).

Clearly, $[E : F]$ is finite. We will see in Section 2.5 that for any field F and any polynomial $f \in F[X] \setminus F$ there exists a splitting field of f over F .

Finite Field

First of all, we define the concept of *prime field* and *prime subfield*. The *prime subfield* of a field F denoted by $P(F)$, is the intersection of all subfields of F . A *prime field* is a field which has no proper subfields. One can define the characteristic of a field F using the notion of prime subfield as follows:

$$\text{Char}(F) = \begin{cases} p > 0 & \text{if } P(F) \cong \mathbb{Z}_p \\ 0 & \text{if } P(F) \cong \mathbb{Q}. \end{cases}$$

Now if F is a finite field, then clearly the characteristic of F is $p > 0$. Then $P(F) \cong \mathbb{Z}_p$. Since $F/P(F)$ is a finite extension, say $[F : P(F)] = n$, we have $|F| = p^n$, considering F as a vector space over $P(F)$.

Conversely, let $p > 0$ be a prime number, and let n be a positive integer. Then there exists a field F with p^n elements. We take the splitting field of the polynomial $f = X^{p^n} - X \in \mathbb{Z}_p[X]$. Clearly, this polynomial is separable since we have that $f' = p^n X^{p^n-1} - 1 \neq 0$. So, f has p^n distinct roots in any splitting field of F .

Any such field F with p^n elements is also a splitting field of f over $P(F)$ which implies that any two finite fields are isomorphic if and only if they have the same number of elements. Hence, for any power of a prime number q , there exists a field, that will be denoted as \mathbb{F}_q , with $|\mathbb{F}_q| = q$, which is unique up to isomorphism. We will denote \mathbb{Z}_p by \mathbb{F}_p . Also for any finite field \mathbb{F}_q and any $n \in \mathbb{N}^*$, we have that \mathbb{F}_q is a subfield of \mathbb{F}_{q^n} .

Algebraically Closed Extension

Algebraically closed field. A field F is said to be *algebraically closed* if it satisfies one of the following equivalent conditions.

- (1) Every irreducible polynomial over F is linear.
- (2) Every nonconstant polynomial over F has at least one root in F .

- (3) Every nonconstant polynomial in $F[X]$ splits over F .
- (4) There exists no proper overfield E of F such that E is an algebraic extension of F .

Steinitz's Extension Theorem. Let E/F be an algebraic extension, let Ω be an algebraically closed field, and let $\sigma : F \longrightarrow \Omega$ be a field homomorphism. Then σ can be extended to a field homomorphism $\tau : E \longrightarrow \Omega$.

Algebraic closure. An *algebraic closure* of a field F is an overfield E of F such that E is algebraically closed and E/F is an algebraic extension.

Any field F has an algebraic closure which is unique up to an F -isomorphism. An algebraic closure of F is denoted by \overline{F} .

The following facts follow from Steinitz's Extension Theorem.

(1) If \overline{F} is a fixed algebraic closure of F , and E/F is any algebraic extension, then there exists an F -homomorphism $\tau : E \longrightarrow \overline{F}$, which is necessarily injective, and extends the canonical injection $j : F \longrightarrow \overline{F}$. Identifying E with $\tau(E)$, we can assume that any algebraic extension of F can be considered as a subfield of \overline{F} .

(2) If E/F is an algebraic extension, then every F -automorphism of E can be extended to an F -automorphism of \overline{F} .

Normal Extension

Conjugate elements. Let F be a field, let \overline{F} be a fixed algebraic closure of F , and let $x, y \in \overline{F}$. Then, x and y are called *conjugate elements over F* if one of the equivalent conditions is satisfied.

- (1) There exists an F -automorphism σ of \overline{F} such that $\sigma(x) = y$.
- (2) There exists an F -isomorphism $\tau : F(x) \longrightarrow F(y)$ such that $\tau(x) = y$.
- (3) $\text{Min}(x, F) = \text{Min}(y, F)$.

Equivalent definitions. An extension E/F (where $E \subseteq \overline{F}$) is said to be normal, if it is algebraic, and satisfies one of the following equivalent conditions.

- (1) Whenever f is an irreducible polynomial in $F[X]$ then either f splits over E , or f has no roots in E .
- (2) The minimal polynomial of each element of E splits over E .
- (3) $\sigma|_E \in \text{Gal}(E/F)$ for every $\sigma \in \text{Gal}(\overline{F}/F)$.
- (4) For each $x \in E$, all conjugates of x over F belong to E .
- (5) $\sigma(E) \subseteq E$ for every F -homomorphism $\tau : E \rightarrow \overline{F}$.

Now we list some important properties of normal extensions.

- (1) Let $F \subseteq K \subseteq E$ be a tower of fields. If E/F is a normal extension then so is also E/K .
- (2) Let $(E_j/F)_{j \in I}$ be a family of normal extensions. Then the extension $(\bigcap_{j \in I} E_j)/F$ and $F(\bigcup_{j \in I} E_j)/F$ are also normal, that is, the meet and the compositum of any family of normal extensions is normal.
- (3) For any algebraic extension E/F there exists a “least” normal extension \tilde{E}/F containing E/F as a subextension, where \tilde{E} is the intersection of all subfields N of \overline{F} containing E such that N/F is a normal extension. The extension \tilde{E}/F is called the *normal closure* of the extension E/F . The *normal closure* of a finite extension is also a finite extension.

Separable Extension

Multiple Root. Let f be a polynomial in $F[X] \setminus F$ having a root u in F . If $(X - u)^m$ divides f , but $(X - u)^{m+1}$ does not divide f , then the number m is called the *multiplicity* of u . We say that u is a *multiple root* if $m > 1$ and a *simple root* if $m = 1$.

Definition 2.3.11. Let $f = a_0 + a_1X + \dots + a_nX^n \in F[X]$. We define the derivative f' of f by

$$f' = a_1 + 2a_2X + \dots + na_nX^{n-1}$$

where $ka_k = a_k + \dots + a_k$ (k times). Thus, we obtain a map called differentiation

$$D : F[X] \longrightarrow F[X], f \mapsto f'.$$

This map has the following properties:

$$(1) (f + g)' = f' + g',$$

$$(2) (af)' = af',$$

$$(3) (fg)' = fg' + gf',$$

for every $f, g \in F[X]$, and $a \in F$.

□

Proposition 2.3.12. For an irreducible polynomial $f \in F[X]$, the followings are equivalent.

(1) In every splitting field of f over F , f factors into distinct linear factors.,

(2) In some splitting field of f over F , f factors into distinct linear factors.

(3) $f' \neq 0$.

Proof. (1) \implies (2) is obvious.

(2) \implies (3) : Suppose that $f' = 0$. Then for any root a of f , $X - a$ divides both f and f' . Then $f = h \cdot (X - a)$ and $f' = h' \cdot (X - a) + h$. Since $(X - a) \mid f'$, clearly we have $(X - a) \mid h$. So, $(X - a)^2$ divides f , which is contrary to our assumption.

(3) \implies (1) : Suppose that f has repeated factors in some splitting field E of f over F . Let $(X - a)^2$ divides f in $E[X]$. We know that $(X - a)$ divides both f and

f' . But f is irreducible over F and f' is a polynomial which has a lower degree than that of f . Then, $\gcd(f, f') = 1$, so there exists some polynomials $r, s \in F[X]$ such that $rf + sf' = 1$. Now evaluating this equation at a , we obtain $0 = 1$, which is a contradiction. Hence, f factors into distinct linear factors in any splitting field of f over F . \square

Definition 2.3.13. Let f be an irreducible polynomial over F . We say that f is separable over F , if one of the equivalent statements of Proposition 2.3.12 hold. An algebraic element u is said to be separable over F if its minimal polynomial is separable over F . An algebraic extension E/F is separable over F if every element of E is separable over F . A polynomial is said to be separable over F if every irreducible factor in $F[X]$ is separable. \square

Now we list some basic properties of separable extensions.

- (1) A field F is perfect if and only if every algebraic extension of F is separable. In particular, any algebraic extension of a field of characteristic 0 or of a finite field is a separable extension.
- (2) Let $F \subseteq K \subseteq E$ be a tower of fields. Then E/F is a separable extension if and only if both K/F and E/K are separable.

Separable Degree

Let F be a field of characteristic $p > 0$, and let f be an irreducible polynomial in $F[X]$. Then there exists a unique number $e \in \mathbb{N}$ such that $f \in F[X^{p^e}]$ but $f \notin F[X^{p^{e+1}}]$, and we write $f = g(X^{p^e})$ for some $g \in F[X]$. The following statements hold.

- (1) g is irreducible and separable over F .
- (2) All roots of f in \overline{F} have the same multiplicity equal to p^e , and the degree of g is equal to the number of distinct roots in \overline{F} of f , and so

$$\deg(f) = p^e \cdot \deg(g).$$

The positive integers $\deg(g)$ and p^e are called the *separable degree* of f and the *degree of inseparability* of f , respectively.

If E/F is an extension and $u \in E$ is an algebraic element, then we define the *separable degree* of u over F (resp. the *degree of inseparability*) as the *separable degree* of the minimal polynomial of u over F . One can also define the *separable degree* of an extension E/F as being the number of all F -homomorphisms from E into \overline{F} ; it is denoted by $[E : F]_s$. Let E/F be an extension with F a field of characteristic $p > 0$, let $u \in E$ be algebraic over F , having the degree of inseparability p^e . Then $[F(u) : F]_s$ is equal to the separable degree of u over F , and

$$[F(u) : F] = p^e \cdot [F(u) : F]_s.$$

Throughout this Thesis F denotes an arbitrary field and Ω a fixed algebraically closed field containing F as a subfield; any overfield of F is a subfield of Ω . For any $n \in \mathbb{N}^*$, ζ_n denotes a primitive n -th root of unity over F , that is, a generator of the cyclic group $\mu_n(\Omega) = \{x \in \Omega \mid x^n = 1\}$. We denote by $\mu(F)$, the set of all roots of unity in F . Then we have

$$\mu_n(F) \leq \mu(F) \leq F^*,$$

for all $n \in \mathbb{N}^*$. We also have

$$\mu(F) = \bigcup_{k \geq 1} \mu_k(F) \text{ and } \mu_m(F) \subseteq \mu_n(F) \text{ if } m \mid n.$$

2.4 Ruler and Compass Constructions

In this part we will use one of our previous results which is about calculating the degree of a field extension. We apply that result to some problems which come from classical Greek geometry.

In the ancient Greek geometry, people restricted the instruments that they used, and they obtained a wide range of geometric constructions using only rulers and compasses. With these two instruments, it is possible to divide a line segment into

many equal parts, to bisect an angle and to draw parallel lines. Also given any polygon of a certain area, it is possible to construct a square of equal area of the polygon. There are many other constructions obtained in this way, but there are also some constructions for which these two instruments are inadequate. Some of the well known constructions that the Greeks could not construct using only rulers and compasses are: *duplicating the cube*, *trisecting the angle*, *squaring the circle*. In other words, the first problem asks for constructing a cube twice the volume of a given cube, the second one asks for constructing an angle one third the size of a given angle, and the last one asks for constructing a square of area equal to the area of a given circle.

Before providing the proofs for the impossibility of the three problems above, we are going to formalize the idea of the ruler and compass construction. Let P_0 be a set of points in the Euclidean plane \mathbb{R}^2 . Then using a ruler, we can draw a straight line through any two points of P_0 , and using a compass, we can draw a circle whose center is a point of P_0 , and whose radius is equal to the distance between some pair of points in P_0 .

Definition 2.4.1. *The points of intersections of any two distinct lines or circles drawn using a ruler and a compass are said to be constructible in one step from the set P_0 . More generally, a point $r \in \mathbb{R}^2$ is constructible from P_0 if there is a finite sequence $r_1, r_2, \dots, r_n = r$ of points of \mathbb{R}^2 , such that for each $j = 1, 2, \dots, n$ the point r_j is constructible in one step from the set $P_0 \cup \{r_1, r_2, \dots, r_{j-1}\}$. \square*

Example 2.4.2. Suppose we are given two points $p_1, p_2 \in \mathbb{R}^2$. Now we are going to construct the midpoint of the line segment determined by these two points.

1. Using a ruler, we can draw the line that passes through the points p_1 and p_2 , namely, p_1p_2 .
2. Using a compass, we can draw the circle whose center is p_1 and whose radius is p_1p_2 .
3. Also we can draw the circle whose center is p_2 and whose radius is p_1p_2 .
4. Now let r_1 and r_2 be the intersection points of these circles.
5. Using the ruler, we draw the line r_1r_2 .

6. Now let r_3 be the intersection point of the lines p_1p_2 and r_1r_2 .

Then the sequence of points r_1, r_2, r_3 provides a construction of the midpoint of the line p_1p_2 . \square

Since a line is determined by any two distinct points on itself and a circle is determined by its center and a point on itself, all the traditional geometrical constructions of Euclidean geometry fall into the scope of Definition 2.4.1.

We are going to see that the limitations of the ruler and compass constructions is related to the degree of some field extension.

To each stage of the construction, we associate a subfield of \mathbb{C} , generated by the coordinates of the points constructed. So, let K_0 be generated by the x - and y -coordinates of the points in P_0 . Then clearly, K_0 is a subfield of \mathbb{R} . If $r_j = (x_j, y_j)$, then we can define K_j to be the field obtained from K_{j-1} by adjoining x_j and y_j to K_{j-1} . We can write this as follows:

$$K_j = K_{j-1}(\{x_j, y_j\}) = K_{j-1}(x_j, y_j).$$

Then we have a tower of subfields,

$$K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \mathbb{R}.$$

After doing some calculations, we can see that x_j and y_j in K_j are roots of some quadratic polynomials over K_{j-1} . In order to do that, we have to consider three cases: line meeting circle, line meeting line and circle meeting circle.

We are going to derive a criterion for constructibility and use Proposition 2.3.5.

Proposition 2.4.3. *If $r = (x, y)$ is constructible from a subset P_0 of \mathbb{R}^2 , and K_0 is the subfield of \mathbb{R} generated by the coordinates of the points of P_0 , then the degrees*

$$[K_0(x) : K] \text{ and } [K_0(y) : K]$$

are powers of 2.

Proof. Using the result which we have mentioned above, we obtain

$$[K_{j-1}(x_j) : K_{j-1}] = 1 \text{ or } 2, \text{ similarly } [K_{j-1}(y_j) : K_{j-1}] = 1 \text{ or } 2.$$

Then from Proposition 2.3.5, we have

$$[K_{j-1}(x_j, y_j) : K_{j-1}] = [K_{j-1}(x_j, y_j) : K_{j-1}(x_j)] \cdot [K_{j-1}(x_j) : K_{j-1}] = 1, 2 \text{ or } 4.$$

But since we have defined K_j as $K_{j-1}(x_j, y_j)$, we can say that $[K_j : K_{j-1}]$ is a power of 2. Clearly, $[K_n : K_0]$ is a power of 2. Since

$$[K_n : K_0] = [K_n : K_0(x)] \cdot [K_0(x) : K_0],$$

we have $[K_0(x) : K_0]$ is a power of 2. Similarly, $[K_0(y) : K_0]$ is a power of 2. \square

If we take in the above proposition r to be a real number and $P_0 = \mathbb{Q}$, then we have a nice result which says that any constructible real number is algebraic over \mathbb{Q} and its degree over the rational numbers is a power of 2.

Now we can solve our geometric problems, which we mentioned at the beginning of this section, using algebraic notions.

Squaring the circle:

The problem is to construct a square whose area is equal to that of a circle of radius 1, using a ruler and a compass. This is equivalent to constructing the real number $\sqrt{\pi}$. But this is impossible since from our last result we know that a constructible real number should be algebraic over \mathbb{Q} , whereas the number π is transcendental over \mathbb{Q} .

Duplicating the cube:

The problem is to construct a cube whose volume is 2, using a ruler and a compass. But this time such a construction is equivalent to constructing the real number $\sqrt[3]{2}$. This number is algebraic over \mathbb{Q} , but its degree over \mathbb{Q} is 3, by the theorem below. ²

Trisecting the angle $\pi/3$:

²If g is a monic polynomial (the polynomial is monic if the leading coefficient is 1) with integer coefficients then any rational root of g is an integer: Suppose that m/n is a root of g with $\gcd(m, n) = 1$. Let $g = a_0 + a_1X + \dots + a_{k-1}X^{k-1} + X^k$, so we have $a_0 + a_1m/n + \dots + a_{k-1}(m/n)^{k-1} + (m/n)^k = 0$. Then, $a_0n^k + a_1m(n)^{k-1} + \dots + a_{k-1}(m)^{k-1}n + (m)^k = 0$. But this implies that $n|m$ which is a contradiction. Hence any rational root of g should be integer.

It is easy to construct the angle $\pi/3$, starting from the points $(0, 0)$ and $(1, 0)$. To trisect the angle $\pi/3$, we again start from the points $(0, 0)$ and $(1, 0)$. In order to do that, we have to construct the point $(\alpha, 0)$ where $\alpha = \cos(\pi/9)$. If we construct the point $(\alpha, 0)$, then we can also construct the point $(\beta, 0)$ where $\beta = 2\cos(\pi/9)$. From trigonometry we know that

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

If we put $\theta = \pi/9$, then $\cos(3\theta) = 1/2$. Now β satisfies the cubic equation

$$\beta^3 - 3\beta - 1 = 0.$$

But $f = X^3 - 3X - 1$ is irreducible over \mathbb{Q} . Suppose that f is reducible over \mathbb{Q} . Then f has a root, a in \mathbb{Q} . By the theorem which was used in the impossibility proof of the duplicating the cube, a would be an integer dividing 1. But ± 1 is not a root of f , so f is irreducible over \mathbb{Q} . So, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, which is not a power of 2.

2.5 Splitting Fields

In this section our aim is to show that every polynomial $f \in F[X] \setminus F$ has a splitting field over F and any two splitting fields of f over F are isomorphic.

Proposition 2.5.1. *If F is a field and $h \in F[X]$ is irreducible, then $F[X]/(h)$ is a field containing (an isomorphic copy of) F and a root of h .*

Proof. Since h is irreducible, the principal ideal $I = (h)$ is a nonzero prime ideal. We know that $F[X]$ is a PID, and so I is a maximal ideal. Hence, $E = F[X]/I$ is a field. Clearly, $a \mapsto a + I$ is an isomorphism from F onto the subset $\{a + I : a \in F\}$ of E . Let $\theta = X + I \in E$. Our aim is to show that θ is a root of h , that is $h(\theta) = I$, since I is the identity element of $F[X]/I$. Let $h = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$, where $a_i \in F$. According to the isomorphism above, we can identify the elements of F with

the elements of the set $\{a + I : a \in F\}$. So,

$$\begin{aligned} h(\theta) &= (a_0 + I) + (a_1 + I)\theta + \dots + (a_n + I)\theta^n, \\ &= (a_0 + I) + (a_1 + I)(X + I) + \dots + (a_n + I)(X + I)^n \\ &= (a_0 + I) + (a_1X + I) + \dots + (a_nX^n + I) \\ &= a_0 + a_1X + \dots + a_nX^n + I \\ &= h + I = I. \end{aligned}$$

Thus, $\theta \in E = F[X]/I$ is a root of h . □

Theorem 2.5.2. *Let $f \in F[X]$, where F is a field. Then there exists a splitting field E containing F .*

Proof. We are going to prove this theorem by induction on the degree of the polynomial f . If $\deg(f) = 1$, then f is linear. So we can take $E = F$, since f splits over F . If $\deg(f) > 1$, then we can write $f = g \cdot h$ where h is irreducible. If h is linear and $\deg(g) < \deg(f)$, then by induction hypothesis, there exists a splitting field of g over F . But this splitting field is also a splitting field of f , since h is linear. If $\deg(h) > 1$, then we construct the field $F(u_1)$ by using the above proposition, where u_1 is a root of the polynomial h . By induction hypothesis, we can find a splitting field E of the polynomial $f/(X - u_1)$ over $F(u_1)$. Then we obtain $E = F(u_1)(u_2, u_3, \dots, u_r)$ where u_2, u_3, \dots, u_r are roots of the polynomial $f/(X - u_1)$. Hence, $E = F(u_1, u_2, u_3, \dots, u_r)$. This shows that E is a splitting field of f over F . □

If $\sigma : F \rightarrow L$ is a field homomorphism, then one defines a map

$$\bar{\sigma} : F[X] \rightarrow L[X],$$

$$\bar{\sigma}(a_0 + a_1X + \dots + a_nX^n) = \sigma(a_0) + \sigma(a_1)X + \dots + \sigma(a_n)X^n.$$

If $f = a_0 + a_1X + \dots + a_nX^n$, then $\bar{\sigma}(f)$ will be denoted in the sequel by $\sigma(f)$.

Now we show that any two splitting fields over F of a polynomial $f \in F[X]$ are isomorphic. Firstly, we prove this statement for an irreducible polynomial.

Proposition 2.5.3. *Let F and F_0 be fields with σ an isomorphism of F onto F_0 . Let $f \in F[X]$ be an irreducible polynomial and $\sigma(f) \in F_0[X]$ be the corresponding polynomial. Let $E = F(u)$ and $E_0 = F_0(u_0)$ where u and u_0 are roots of f and $\sigma(f)$ respectively. Then σ can be extended to an isomorphism of E onto E_0 which coincides with σ on F and sends u into u_0 . In this case, the number of such extensions is the same as the number of distinct roots of $\sigma(f)$ in E_0 .*

Proof. Define η from the field $E = F(u)$ to the field $E_0 = F_0(u_0)$ by

$$\eta\left(\sum_{i=0}^n a_i u^i\right) = \sum_{i=0}^n \sigma(a_i) u_0^i.$$

This map is well-defined. Indeed, let $g, h \in F[X]$ be such that $g(u) = h(u)$. So,

$$(g - h)(u) = 0.$$

Since f is irreducible and u is a root of f , by Proposition 2.3.5 part (1), we deduce that $f \mid (g - h)$. We have $g - h = f \cdot k$ with $k \in F[X]$. Applying σ to this equation, we obtain

$$\sigma(g - h) = \sigma(fk).$$

Since σ is an isomorphism, $\sigma(g) - \sigma(h) = \sigma(f)\sigma(k)$. But this implies that

$$\sigma(f) \mid (\sigma(g) - \sigma(h)).$$

Since u_0 is a root of $\sigma(f)$, u_0 is also a root of $\sigma(g) - \sigma(h)$, that is, $\sigma(g)(u_0) = \sigma(h)(u_0)$.

We obtain

$$\eta(g(u)) = \eta(h(u)).$$

Hence, this map is well-defined. It can easily be shown that this map is one to one and onto. Thus, this map is an isomorphism. It sends u into u_0 and agrees with σ on F . It is clear that the number of such extensions is the same as the number of distinct choices of u_0 , hence the number of distinct roots of $\sigma(f)$ in E_0 . \square

Now we are going to prove the next result which is more general than this one.

Proposition 2.5.4. *Let F and F_0 be fields with σ an isomorphism of F onto F_0 . Let $f \in F[X]$ and $\sigma(f) \in F_0[X]$ the corresponding polynomial. Let E and E_0 the splitting fields of f and $\sigma(f)$ respectively. Then σ can be extended to an isomorphism of E onto E_0 . If f is separable over F , then there are exactly $[E : F]$ extensions of σ .*

Proof. We prove this proposition by induction on $[E : F]$. If $[E : F] = 1$, then $E = F$ and f factors into distinct linear factors over E , that is,

$$f = \prod (X - u_i)$$

in $F[X]$. Now we apply the isomorphism σ and obtain

$$\sigma(f) = \prod (X - \sigma(u_i))$$

in $F_0[X]$. Hence, $\sigma(u_i)$ are the roots of $\sigma(f)$. E_0 is generated over F_0 by the roots of $\sigma(f)$ since it is a splitting field of $\sigma(f)$. Therefore, $E_0 = F_0$, and there is only one extension.

Now assume $[E : F] > 1$. Then f is not a product of linear factors in $F[X]$. So, we may assume that f has an irreducible factor, say g of degree bigger than 1. Then, $\sigma(g)$ is a root of $\sigma(f)$. Let u be a root of g (clearly, $u \notin F$, otherwise g would be reducible over F). Then, by Proposition 2.5.3, the isomorphism σ can be extended to an isomorphism of $F(u)$ onto $F_0(\sigma(u))$. It is easy to see that E is a splitting field of f over $F(u)$ and E_0 is a splitting field of $\sigma(f)$ over $F_0(\sigma(u))$. We have

$$[E : F(u)] < [E : F],$$

since $u \notin F$. So, by induction hypothesis, σ can be extended to an isomorphism of E onto E_0 .

Now we are going to show that there are exactly $[E : F]$ extensions of σ , where f is a separable polynomial over F . We proceed again by induction on $[E : F]$. If $[E : F] > 1$ then there exists an irreducible factor of f of degree bigger than 1. Let $f = p \cdot q$, where p is irreducible over F of degree $d > 1$. Let u be a root of p . Then, $\sigma(u)$ is a root of $\sigma(p)$.

By Proposition 2.5.3, σ can be extended to an isomorphism of E onto E_0 . We know that $\sigma(f)$ is separable since f is separable and σ is one to one. Also, $\sigma(p)$ is separable, which means that it has exactly d roots. By Proposition 2.5.3, there are exactly d isomorphisms extending σ , one for each root of p . Clearly, E is a splitting field of f over $F(u)$ and E_0 is a splitting field of $\sigma(f)$ over $F_0(\sigma(u))$. We know

$$[E : F(u)] = [E : F]/[F(u) : F] = [E : F]/d < [E : F].$$

By induction hypothesis, for each of the d isomorphisms, we have exactly $[E : F]/d$ extensions to E . Therefore, σ has exactly $d \cdot [E : F]/d$ extensions, which is $[E : F]$. \square

Example 2.5.5. Let $F = \mathbb{Q}$ and $f = (X^2 - 2)(X^2 - 3)$. Clearly, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of f since E is generated over \mathbb{Q} by $\sqrt{2}$ and $\sqrt{3}$ and the roots of f are $\pm\sqrt{2}$ and $\pm\sqrt{3}$. Now we calculate the degree of E over F . $\sqrt{3}$ is of degree 2 over \mathbb{Q} , since its minimal polynomial is $X^2 - 3$ ($X^2 - 3$ is irreducible over \mathbb{Q} by a theorem which is discussed in the impossibility proof of duplicating the cube). So the degree of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ is at most 2.

If $X^2 - 3$ is also irreducible over $\mathbb{Q}(\sqrt{2})$, then the degree of this extension is exactly 2. Since the degree of $X^2 - 3$ is 2, this polynomial is reducible over $\mathbb{Q}(\sqrt{2})$, if it has a root in $\mathbb{Q}(\sqrt{2})$, which is $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then, using the fact that $\{1, \sqrt{2}\}$ generates $\mathbb{Q}(\sqrt{2})$, we obtain $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Squaring both sides, we obtain $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$.

If $ab \neq 0$, then $\sqrt{2}$ should be a rational number, but this is a contradiction. If $b = 0$, then this implies that $\sqrt{3}$ should be a rational number, which again leads to a contradiction. If $a = 0$, then we have $\sqrt{3} = b\sqrt{2}$. Multiplying both sides with $\sqrt{2}$, we obtain the result that $\sqrt{6}$ is a rational number, but this is again a contradiction. Hence, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Using Proposition 1.2.5, we have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. We can easily see that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ generates E . \square

2.6 Foundations of Galois Theory

Now after we have gathered all the required tools, we can start to investigate Galois Theory.

Definition 2.6.1. *The Galois group of a polynomial $f \in F[X]$ is the Galois group of E/F , where E is a splitting field of f . \square*

Clearly, $\text{Gal}(E/F)$ is a subgroup of $\text{Aut}(E)$, where $\text{Aut}(E)$ denotes the set of all automorphisms of E . We can easily see that $\text{Aut}(E)$ forms a group under the composition of mappings.

Now we are going to prove a result which will be used throughout the Thesis.

Lemma 2.6.2. *Let $f \in F[X]$, and let E/F be a splitting field of f over F . If we have $\sigma \in \text{Gal}(E/F)$ and if u is a root of f , then $\sigma(u)$ is also a root of f .*

Proof. Let $f = b_0 + b_1X + b_2X^2 + \dots + b_nX^n \in F[X]$. Since u is a root of f , we have $b_0 + b_1u + b_2u^2 + \dots + b_nu^n = 0$. Applying σ to both sides of the equation, we obtain $\sigma(b_0) + \sigma(b_1)\sigma(u) + \sigma(b_2)\sigma(u)^2 + \dots + \sigma(b_n)\sigma(u)^n = 0$. But σ fixes the elements of F pointwise, so $\sigma(b_i) = b_i$ for all $1 \leq i \leq n$. Hence, $\sigma(u)$ is a root of f . \square

In particular, let $E = F(u)$, and let u be algebraic over F . Now put $g = \text{Min}(u, F)$. Then, for $\sigma \in \text{Gal}(E/F)$, we have that $\sigma(u)$ is also a root of g .

Now in the next examples we determine the Galois groups of some extensions.

Example 2.6.3. Consider the field extension \mathbb{C}/\mathbb{R} . It is easy to see that $\mathbb{C} = \mathbb{R}(i)$. So, we deduce that \mathbb{C} is a splitting field of the polynomial $f = X^2 + 1 \in \mathbb{R}[X]$, since the roots of f are $\pm i$. The degree of the extension $\mathbb{R}(i)/\mathbb{R}$ is 2, since the minimal polynomial of i over \mathbb{R} is $X^2 + 1$, that is $[\mathbb{C} : \mathbb{R}] = 2$.

By Definition 2.6.1, the Galois group of f is $\text{Gal}(\mathbb{C}/\mathbb{R})$. Let $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$ and let u be a root of f . Then, $\sigma(u)$ is also a root of f by Lemma 2.6.2. This means that σ sends roots of f to roots of f . But f has exactly two roots which are $\pm i$. Then, we have exactly two automorphisms in $\text{Gal}(\mathbb{C}/\mathbb{R})$. These are $\sigma_1 : i \mapsto i$, i.e., $\sigma_1 = 1_{\mathbb{C}}$ and $\sigma_2 : i \mapsto -i$, i.e., $\sigma_2(a + bi) = a - bi$. Therefore $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{1_{\mathbb{C}}, \sigma_2\}$. \square

Example 2.6.4. Now we determine the Galois group of the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. We know that $\sqrt[3]{2}$ is algebraic over \mathbb{Q} and its minimal polynomial is $f = X^3 - 2 \in \mathbb{Q}[X]$. The other roots of this polynomial are $\varepsilon\sqrt[3]{2}$ and $\varepsilon^2\sqrt[3]{2}$, where ε is a complex cube root of unity. But these roots of f do not belong to $\mathbb{Q}(\sqrt[3]{2})$. Hence, Lemma 2.6.2 shows that $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ consists only of the identity automorphism. \square

Proposition 2.6.5. *If $f \in F[X]$ is a separable polynomial and if E/F is its splitting field, then $|\text{Gal}(E/F)| = [E : F]$.*

Proof. In Proposition 2.5.4, if we take $F = F_0$ and $E = E_0$, and $\sigma : F \rightarrow F$ as the identity mapping on F , then there are exactly $[E : F]$ automorphisms of E fixing F . In other words $|\text{Gal}(E/F)| = [E : F]$. \square

2.6.1 Galois Correspondence

Let E/F be a field extension with Galois group $\text{Gal}(E/F) = G$. In this section our aim is to set up a correspondence between the subgroups of G and the intermediate fields lying between E and F .

Firstly, we are going to define a set which will play an important role in the subject.

Let H be a subgroup of G . $\text{Fix}(H)$ denotes the set of all elements of E which are fixed by every automorphism in H , i.e.,

$$\text{Fix}(H) = \{a \in E \mid \sigma(a) = a, \sigma \in H\}.$$

It is easy to see that this set is a subfield of E , so it is natural to call this set as the fixed subfield of E under H .

Now we can define two maps such that

$$\alpha : \underline{\text{Intermediate}}(E/F) \longrightarrow \underline{\text{Subgroups}}(G), \quad \alpha(K) = \text{Gal}(E/K)$$

$$\beta : \underline{\text{Subgroups}}(G) \longrightarrow \underline{\text{Intermediate}}(E/F), \quad \beta(H) = \text{Fix}(H).$$

The first map is from the set of intermediate fields of E containing F into the set of subgroups of the Galois group G and the second map is from the subgroups of G into the set of intermediate fields of the extension E/F .

We list some of the basic properties of these two maps:

(i) If $F \subseteq K \subseteq L \subseteq E$, then $\text{Gal}(E/K) \supseteq \text{Gal}(E/L)$

(ii) If $1 \subseteq J \subseteq H \subseteq G$, then $\text{Fix}(J) \supseteq \text{Fix}(H)$

(iii) $\text{Fix}(E/\text{Fix}(G)) \supseteq F$

(iv) $\text{Gal}(E/\text{Fix}(G)) \supseteq G$.

To show that the first statement holds, let $F \subseteq K \subseteq L \subseteq E$ and $\sigma \in \text{Gal}(E/L)$. So $\sigma(x) = x$, for all $x \in L$. But $L \supseteq K$, so $\sigma(x) = x$ for all $x \in K$, which means that $\sigma \in \text{Gal}(E/K)$. Therefore we have $\text{Gal}(E/K) \supseteq \text{Gal}(E/L)$. The other statements can be shown in a similar way.

According to our last result, the above maps between the set of subgroups of G and the set of intermediate fields lying between E and F are inclusion reversing.

From what we have introduced above, we see that the equalities $\text{Gal}(E/E) = 1$ and $\text{Fix}(1) = E$ holds.

It is not always the case that $\text{Fix}(G) = F$. For example, if take $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2})$, then by Example 2.6.4, we have $G = \text{Gal}(E/F) = \{1\}$. Hence, we have $\text{Fix}(G) = E \neq F$. But $F \subseteq \text{Fix}(G)$ always holds, since any element of F is left fixed by any automorphism in G .

Definition 2.6.6. *An algebraic extension E/F is called Galois if $\text{Fix}(G) = F$, that is, G fixes F and nothing more. In other words, E/F is said to be Galois, if for all $u \in E$, $u \notin F$ there exists an F -automorphism σ of E such that $\sigma(u) \neq u$, that is, all elements of E , which do not belong to F , are moved by some automorphism of E . \square*

Now the following result expresses the Galois extensions in a different way.

Proposition 2.6.7. *The following conditions are equivalent for a finite extension E/F with Galois group $G = \text{Gal}(E/F)$.*

(1) $F = \text{Fix}(G)$.

(2) Every irreducible polynomial $p \in F[X]$ with one root in E is separable and has all its roots in E ; that is p splits over E .

(3) E is a splitting field of some separable polynomial $f \in F[X]$.

Proof. (1) \implies (2) : Let $p \in F[X]$ be an irreducible polynomial having a root u in E . Let $u = u_1, u_2, \dots, u_r$ be the distinct images of u under the automorphisms in G .³ Proposition 2.6.2 implies that each u_i is a root of p in E . Then $\deg(p) \geq r$. Let $g \in E[X]$ be such that

$$g = \prod (X - u_i). \quad (2.6.1)$$

Let $\sigma \in G$, so we have $\sigma(u_i) = u_j$ for some $1 \leq i, j \leq r$. Hence, applying σ to the Equation (2.6.1), we obtain $\sigma(g) = g$. But E/F is a Galois extension, which means that G fixes F and nothing more. So, $g \in F[X]$. We know that u is a root of both of the polynomials p and g . Clearly, p is the minimal polynomial of u over F , since p is irreducible over F . Part (1) of Proposition 2.3.8 implies that $p \mid g$, which means that $\deg(p) \leq \deg(g) = r$. But we also have $\deg(p) \geq r$. Hence, $p = g$, which means that p splits over E .

(2) \implies (3) : Suppose that (2) holds. Let $u_1 \in E$ with $u_1 \notin F$. We have that E/F is an algebraic extension, since E/F is finite. Then u_1 is algebraic over F . Let $f_1 \in F[X]$ be its minimal polynomial. Clearly it is irreducible. Then, by hypothesis, we have that f_1 is a separable polynomial which splits over E . Let $K_1 \subseteq E$ be its splitting field. If $K_1 = E$, then we are done.

Otherwise, if $K_1 \neq E$, choose $u_2 \in E$ and $u_2 \notin K_1$. Then, u_2 has also a minimal polynomial, say $f_2 \in F[X]$, which is irreducible. By hypothesis, f_2 is separable and splits over E . Let $K_2 \subseteq E$ be a splitting field of $f_1 f_2$, which is separable and splits over E . If $K_2 = E$, then we are done. If not, we can continue in this way. But we have to stop somewhere since the extension E/F is finite.⁴ Hence, $E = K_m$ for some m . Therefore E is a splitting field of some separable polynomial.

³ E/F is a finite extension, so, this implies that $|G| < \infty$.

⁴ $\text{Gal}(E/F)$ is finite hence it has finitely many subgroups. After proving The Fundamental Theorem of Finite Galois Theory we can say that E/F has also finitely many intermediate fields.

(3) \implies (1) : Suppose that (3) holds. Then E is a splitting field of some separable polynomial $f \in F[X]$. Theorem 2.6.5 implies that $|G| = |\text{Gal}(E/F)| = [E : F]$. It is easy to see that $F \subseteq \text{Fix}(G) \subseteq E$. E is also a splitting field of f over $\text{Fix}(G)$ and

$$\text{Gal}(E/\text{Fix}(G)) = \text{Gal}(E/F).$$

Using Theorem 2.6.5 again for the field extension $E/\text{Fix}(G)$, we have

$$|\text{Gal}(E/\text{Fix}(G))| = [E : \text{Fix}(G)].$$

But $F \subseteq \text{Fix}(G) \subseteq E$ implies that

$$[E : F] = [E : \text{Fix}(G)] \cdot [\text{Fix}(G) : F].$$

Then $[\text{Fix}(G) : F] = 1$, which means that $\text{Fix}(G) = F$. □

Now we state and prove a more general version of Proposition 2.6.7.

Proposition 2.6.8. *Let E be an extension field of F . Then the followings conditions on E/F are equivalent.*

- (1) E is a splitting field over F of a separable polynomial f .
- (2) $F = \text{Fix}(G)$ for some finite subgroup of automorphisms of E .
- (3) The extension E/F is finite, normal and separable.

Moreover, if E and F are as in (1) and $G = \text{Gal}(E/F)$, then $F = \text{Fix}(G)$; and if G and F are as in (2), then $G = \text{Gal}(E/F)$.

Proof. (1) \implies (2) : Assuming (1), we can say that E/F is finite. The remaining part of the proof will be similar to that of (3) \implies (1) of Proposition 2.6.7. We have also proven the first of the supplementary statements above, in the previous theorem.

(2) \implies (3) : By Artin's Lemma below, $[E : F] \leq |G|$, but $|G| < \infty$. So, E/F is finite. Now assume (2). Let $p \in F[X]$ be an irreducible polynomial having a root $u \in E$. Now using a similar argument in the proof of (1) \implies (2) of Proposition 2.6.7,

we can prove that p splits over E and has all its roots in E . Then, we can say that E/F is normal and separable.

(3) \implies (1) : Since E is finite dimensional over F , we can write $E = F(r_1, r_2, \dots, r_k)$, where r_i is algebraic over F , for all $1 \leq i \leq k$. Let f_i be the minimal polynomial of r_i over F , for all $1 \leq i \leq k$. By hypothesis, each f_i splits over E . But this implies that $f = \prod_{i=1}^k f_i$ is separable and $E = F(r_1, r_2, \dots, r_k)$ is a splitting field of f over F .

Now we prove the second of the supplementary statements. We know that

$$|\text{Gal}(E/F)| = [E : F].$$

Since $G \subseteq \text{Gal}(E/F)$, we have $|G| \leq [E : F]$. But from Artin's Lemma below, we have $[E : F] \leq |G|$. Therefore,

$$|G| = [E : F] = |\text{Gal}(E/F)|.$$

Hence, $G = \text{Gal}(E/F)$. □

Lemma 2.6.9. (Artin) *Let G be a finite group of automorphisms of a field E and let $F = \text{Fix}(G)$. Then $[E : F] \leq |G|$.*

Proof. Let $|G| = n$. If we can show that any $m > n$ elements of E are linearly dependent over F , then we are done. We use a result from linear algebra on linear equations which says: *Any system of n homogenous linear equations in $m > n$ unknowns with coefficients in a field E , has a nontrivial solution in E .*

Let

$$G = \{\alpha_1 = 1, \alpha_2, \dots, \alpha_n\}$$

be a finite set of automorphisms of E and let $u_1, u_2, \dots, u_m \in E$ where $m > n$. Then, the above result on linear equations implies that we have a nontrivial solution of the system of n linear equations

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_i(u_j) x_j = 0 \tag{2.6.2}$$

in m unknowns. We pick one of such solutions, say (b_1, b_2, \dots, b_m) , where the number of nonzero terms is minimum. With possible reordering, we may assume that $b_1 \neq 0$.

If we multiply the solution (b_1, b_2, \dots, b_m) with b_1^{-1} , then we have a solution with the first entry equals to 1. Hence, we may assume that $b_1 = 1$.

Now we claim that all $b_i \in F = \text{Fix}(G)$. Suppose that for some j , $b_j \notin F$. Without loss of generality, for $j = 2$, let $b_2 \notin F$. Then there exists some $\alpha_k \in G$ such that $\alpha_k(b_2) \neq b_2$. Now applying α_k to the system of equations

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_i(u_j) b_j = 0,$$

we obtain

$$\sum_{i=1}^n \sum_{j=1}^m (\alpha_k \alpha_i)(u_j) \alpha_k(b_j) = 0.$$

But $(\alpha_k \alpha_1, \alpha_k \alpha_2, \dots, \alpha_k \alpha_n)$ is a permutation of $(\alpha_1, \alpha_2, \dots, \alpha_n)$. Then, we have

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_i(u_j) \alpha_k(b_j) = 0.$$

Thus, $(1, \alpha_k(b_2), \dots, \alpha_k(b_m))$ is also a solution of the system of equations (2.6.2).

If we subtract this solution from the solution $(1, b_2, \dots, b_m)$, then we obtain another solution of the system of equations (2.6.2), which is $(0, b_2 - \alpha_k(b_2), \dots, b_m - \alpha_k(b_m))$. Since we have $b_2 \neq \alpha_k(b_2)$, this new solution is nontrivial and it has a smaller number of nonzero terms than the solution $(1, b_2, \dots, b_m)$ has. But this is a contradiction, since at the beginning, we had picked the solution having the least number of nonzero terms. Hence, all $b_i \in F = \text{Fix}(G)$. Now for $i = 1$, we have $\sum_{j=1}^m u_j x_j = 0$. This shows that $\{u_i \mid 1 \leq i \leq m\}$ is a linearly dependent set over F . Hence,

$$[E : F] \leq |G|.$$

□

Now we are ready to prove *The Fundamental Theorem of Finite Galois Theory*. By this theorem and the Galois Criterion of solvability by radicals, we will understand why “*Equations of higher degree than 4 cannot generally be solved by radicals.*” This theorem also provides the correspondence between the subgroups of G and the intermediate fields lying between E and F , where E/F is a field extension and $G = \text{Gal}(E/F)$.

Theorem 2.6.10. (*Fundamental Theorem of Finite Galois Theory*) Let E/F be a finite Galois extension, and let $G = \text{Gal}(E/F)$. Let $\Gamma = \underline{\text{Subgroups}}(G)$ and let $\Sigma = \underline{\text{Intermediate}}(E/F)$. The maps

$$\Gamma \longrightarrow \Sigma, \quad H \longrightarrow \text{Fix}(H),$$

and

$$\Sigma \longrightarrow \Gamma, \quad K \longrightarrow \text{Gal}(E/K)$$

are inverses and so are bijections of Γ onto Σ and of Σ onto Γ . Moreover, the following properties hold.

$$(1) \quad |H| = [E : \text{Fix}(H)], \quad |G : H| = [\text{Fix}(H) : F], \quad \text{for every } H \in \Gamma.$$

$$(2) \quad H \text{ is normal in } G \iff \text{Fix}(H) \text{ is normal over } F, \text{ and } \text{Gal}(\text{Fix}(H)/F) \cong G/H.$$

Proof. Let H be a subgroup of $G = \text{Gal}(E/F)$. We have $F \subseteq \text{Fix}(G)$ and $F \subseteq \text{Fix}(H)$, so $\text{Fix}(H)$ is a subfield of E containing F . If we apply the second supplementary result of Proposition 2.6.8 to H , then we obtain $\text{Gal}(E/\text{Fix}(H)) = H$. So by part (1) of Proposition 2.6.8 and Lemma 2.6.9 we have

$$|\text{Gal}(E/\text{Fix}(H))| = [E : \text{Fix}(H)] = |H|.$$

Now let K be an intermediate field of the extension E/F . We have

$$\text{Gal}(E/K) \subseteq \text{Gal}(E/F) = G.$$

Also by part (1) of Proposition 2.6.8, E is a splitting field of some separable polynomial over F . Then, it is clear that E is also a splitting field of some separable polynomial over K . Now we apply the first of the supplementary results of Proposition 2.6.8 to the field extension E/K . We obtain

$$K = \text{Fix}(\text{Gal}(E/K)).$$

Now we have shown that the maps between Γ and Σ are inverses of each other, so they are bijections of Γ onto Σ and of Σ onto Γ . Also, the first part of (1) is shown above.

We have $|G| = [E : F] = [E : \text{Fix}(H)] \cdot [\text{Fix}(H) : F] = |H| \cdot [\text{Fix}(H) : F]$ by part (1). Also we know that $|G| = |H| \cdot [G : H]$. So,

$$[G : H] = [\text{Fix}(H) : F].$$

Therefore (1) is proven.

Now we prove part (2). We claim that H is normal in G if and only if we have $\eta(\text{Fix}(H)) = \text{Fix}(H)$, for every $\eta \in G$. Let $h \in \text{Fix}(H)$. We have to show that $\eta(h)$ is fixed under every automorphism in H . Let $\sigma \in H$. So,

$$\sigma(\eta(h)) = (\sigma\eta)(h) = (\eta\eta^{-1}\sigma\eta)(h) = \eta(\eta^{-1}\sigma\eta)(h).$$

But H is normal in G . Hence, $\eta^{-1}\sigma\eta \in H$. Now $(\eta^{-1}\sigma\eta)(h) = h$ implies that

$$\sigma(\eta(h)) = \eta(h).$$

Thus, $\eta(\text{Fix}(H)) \subseteq \text{Fix}(H)$ for every $\eta \in G$. But for $\eta \in G$, $h \in \text{Fix}(H)$ and $\sigma \in H$, we have $\sigma(h) = h$. Clearly,

$$(\eta\sigma\eta^{-1})(\eta(h)) = \eta(h).$$

So, the subgroup $\eta H \eta^{-1}$ corresponds to the subfield $\eta(\text{Fix}(H))$. But H is normal in G , so this implies that $\eta H \eta^{-1} = H$. This shows that $\eta(\text{Fix}(H))$ and $\text{Fix}(H)$ have the same dimension over F . This follows from part (1). Hence $\eta(\text{Fix}(H)) = \text{Fix}(H)$.

Conversely, we show that for all $\eta \in G$, $\eta H \eta^{-1} = H$. Similarly, for $\eta \in G$, $h \in \text{Fix}(H)$ and $\sigma \in H$, we have $\sigma(h) = h$. Clearly, $(\eta\sigma\eta^{-1})(\eta(h)) = \eta(h)$. This shows that the subfield $\eta(\text{Fix}(H))$, which is equivalent to $\text{Fix}(H)$ by hypothesis, corresponds to the subgroup $\eta H \eta^{-1}$. Similarly $\eta H \eta^{-1} = H$, for all $\eta \in G$. This shows that H is a normal subgroup of G . So we have proven our claim.

Now in this case we prove that

$$\text{Gal}(\text{Fix}(H)/F) \cong G/H.$$

For all $\eta \in G$, $\eta(\text{Fix}(H)) = \text{Fix}(H)$, so the restriction $\bar{\eta} = \eta|_{\text{Fix}(H)}$ is an automorphism of $\text{Fix}(H)/F$. Thus, we have the restriction homomorphism which is defined as:

$$\zeta : \text{Gal}(E/F) \longrightarrow \text{Gal}(\text{Fix}(H)/F), \eta \longmapsto \bar{\eta}.$$

The image of ζ , say \overline{G} , is a group of automorphisms in $\text{Fix}(H)$. We have $\text{Fix}(\overline{G}) = F$.

We can write

$$\text{Fix}(\overline{G}) = \{x \in \text{Fix}(H) \mid \eta(x) = x, \eta \in \overline{G}\}.$$

But this set is a subset of $\text{Fix}(G) = F$. Also this set contains F . Hence $\text{Fix}(\overline{G}) = F$. Thus, $\overline{G} = \text{Gal}(\text{Fix}(H)/F)$ by the supplementary result (2) of Proposition 2.6.8. The kernel of the above homomorphism is the set $\{\eta \in G \mid \eta|_{\text{Fix}(H)} = 1\}$. By the Galois correspondence, this is $\text{Gal}(E/\text{Fix}(H)) = H$. Hence, by the Fundamental Theorem of Isomorphism,

$$G/H \cong \overline{G} = \text{Gal}(\text{Fix}(H)/F).$$

Since $F = \text{Fix}(\overline{G})$, we have that $\text{Fix}(H)$ is normal over F by Proposition 2.6.8.

Conversely, suppose that $\text{Fix}(H)$ is normal over F . Since $[E : F]$ is finite, it is an algebraic extension. So, $\text{Fix}(H)/F$ is also an algebraic extension. Let $a \in \text{Fix}(H)$, and let f be the minimal polynomial of a over F . Since $\text{Fix}(H)$ is normal over F , we can say that f splits over $\text{Fix}(H)$. Then,

$$f = (X - a_1)(X - a_2) \dots (X - a_m)$$

where $a = a_i$ for some $i \in \{1, 2, \dots, m\}$ and $a_j \in \text{Fix}(H)$, for all $i \in \{1, 2, \dots, m\}$. For $\eta \in G$, $f(\eta(a))$ is also a root of f by Proposition 2.6.2. But this shows that $\eta(a) = a_j$ for some $j \in \{1, 2, \dots, m\}$. This implies that $\eta(a) \in \text{Fix}(H)$, since $a_j \in \text{Fix}(H)$. Hence, $\eta(\text{Fix}(H)) \subseteq \text{Fix}(H)$. But as we have shown above, this implies that $\eta H \eta^{-1} \subseteq H$ for all $\eta \in G$. Therefore, H is a normal subgroup of G . \square

Now we consider the case where the extension E/F is infinite dimensional. In this case the group $G = \text{Gal}(E/F)$ is equipped with a natural topology.

We define a subset U of G to be open if for each $\sigma \in U$, there exists an intermediate field $K \subseteq E$ such that

(a) The degree $[K : F]$ is finite.

(b) If σ' is another element of G and the restrictions $\sigma|_K$ and $\sigma'|_K$ are equal, then $\sigma' \in U$.

The resulting collection of open sets forms a topology on G , called the *Krull topology*, and G is a topological group under the Krull topology.

Now we state the theorem which explains the Galois correspondence for infinite extensions.

Theorem 2.6.11. (*Galois Correspondence for Infinite Extensions*) *Let E/F be a field extension and $G = \text{Gal}(E/F)$. The correspondence*

$$K \longrightarrow \text{Gal}(E/K)$$

defined for all intermediate fields $F \subseteq K \subseteq E$, is an inclusion reversing bijection between the set of all intermediate fields K and the set of all closed subgroups H of G . Its inverse is the correspondence

$$H \longrightarrow \text{Fix}(H)$$

defined for all closed subgroups H of G . The extension K/F is normal if and only if $\text{Gal}(E/K)$ is a normal subgroup of G , and in this case the restriction map

$$G \longrightarrow \text{Gal}(K/F)$$

has kernel $\text{Gal}(E/K)$.

Now we give some examples in which we use The Fundamental Theorem of Finite Galois Theory.

Example 2.6.12. Let $f = X^2 - 5 \in \mathbb{Q}[X]$. Since the roots of f are $r_1 = \sqrt{5}$, $r_2 = -\sqrt{5}$, we have that $E = \mathbb{Q}(\sqrt{5})$ is a splitting field of the polynomial f . Then the Galois group of f is $\text{Gal}(E/\mathbb{Q})$. Let $G = \text{Gal}(E/\mathbb{Q})$. The \mathbb{Q} -automorphisms of E are,

$$\begin{array}{ll} \sigma_1 : r_1 \longrightarrow r_1 & \sigma_2 : r_1 \longrightarrow r_2 \\ & r_2 \longrightarrow r_1 \\ & r_2 \longrightarrow r_2 \end{array}$$

Then clearly, $G \cong \mathbb{Z}_2$. In Section 2.7, we will also define the Galois group of the extension E/\mathbb{Q} as the permutation group of the set of roots of f . Using this fact we see that σ_1 corresponds to (1) and σ_2 corresponds to (1, 2). Now we have

$$G = \{\sigma_1, \sigma_2\} = \{(1), (1, 2)\} \cong \mathbb{Z}_2.$$

Since f is a separable polynomial and E is a splitting field of f , $|G| = [E : \mathbb{Q}] = 2$. Now we determine the subgroups of G and the corresponding fixed subfields of E .

The subgroups of G	The corresponding fixed subfields
$G_0 = \{(1)\}$	$\text{Fix}(G_0) = \mathbb{Q}(\sqrt{5})$
$G_1 = G$	$\text{Fix}(G) = \mathbb{Q}$

□

Example 2.6.13. Let $f = X^4 - 2 \in \mathbb{Q}[X]$. Let $E \subseteq \mathbb{C}$ be a splitting field of the polynomial f . We can factorize f over E such that

$$f = (X - \xi)(X + \xi)(X - i\xi)(X + i\xi),$$

where $\xi = \sqrt[4]{2}$. So,

$$\alpha_1 = \xi, \alpha_2 = i\xi, \alpha_3 = -\xi, \alpha_4 = -i\xi$$

are the roots of the polynomial f . Then $E = \mathbb{Q}(\xi, i)$. Since E is a splitting field of a separable polynomial f over \mathbb{Q} , E is normal and separable over \mathbb{Q} by Proposition 2.6.8. Also E is finite dimensional over F . We can write

$$[E : \mathbb{Q}] = [\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}].$$

We know that ξ is a root of the polynomial f and f is irreducible over \mathbb{Q} by Eisenstein's Criterion.⁵ Then, f is the minimal polynomial of ξ over \mathbb{Q} . So,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = 4.$$

The minimal polynomial of i over $\mathbb{Q}(\xi)$ is $X^2 + 1$, since $i^2 + 1 = -1 + 1 = 0$ and $i \notin \mathbb{Q}(\xi) \subseteq \mathbb{R}$. This shows that $X^2 + 1$ is irreducible over $\mathbb{Q}(\xi)$. Hence,

$$[\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)] = 2.$$

⁵Eisenstein's Criterion: Let $f = a_0 + a_1X + \dots + a_nX^n$ be a polynomial over \mathbb{Z} . Suppose that there is a prime q such that $q \nmid a_n$, $q|a_i$ for $0 \leq i \leq n-1$ and $q^2 \nmid a_0$. Then f is irreducible over \mathbb{Q} .

Therefore we have

$$[E : \mathbb{Q}] = 8.$$

Now we determine the elements of the Galois group, say $G = \text{Gal}(E/\mathbb{Q})$, of the polynomial f over \mathbb{Q} . Since E is a splitting field of f over \mathbb{Q} and f is a separable polynomial, we have

$$|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 8.$$

So, there are 8 automorphisms in the Galois group by Proposition 2.6.5. Now the table below displays the elements of the Galois group of f over \mathbb{Q} .

automorphism	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
sends i into	i	i	i	i	$-i$	$-i$	$-i$	$-i$
and $\alpha_1 = \xi$ into	α_1	α_2	α_3	α_4	α_1	α_2	α_3	α_4
so, $\alpha_2 = i\xi$ into	α_2	α_3	α_4	α_1	α_4	α_1	α_2	α_3
$\alpha_3 = -\xi$ into	α_3	α_4	α_1	α_2	α_3	α_4	α_1	α_2
$\alpha_4 = -i\xi$ into	α_4	α_1	α_2	α_3	α_2	α_3	α_4	α_1
σ_i can therefore be represented by the permutation	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)

Now we show how to fill some cells of this table, the remaining cells can be filled in a similar way. Consider σ_4 . We are given $\sigma_4(i) = i$ and $\sigma_4(\xi) = \alpha_4 = -i\xi$. Then,

$$\sigma_4(\alpha_2) = \sigma_4(i\xi) = \sigma_4(i)\sigma_4(\xi) = i\alpha_4 = i(-i\xi) = \xi = \alpha_1.$$

$$\sigma_4(\alpha_3) = \sigma_4(-\xi) = -\sigma_4(\xi) = -\alpha_4 = -(-i\xi) = i\xi = \alpha_2.$$

$$\sigma_4(\alpha_4) = \sigma_4(-i\xi) = -\sigma_4(i)\sigma_4(\xi) = -i\alpha_4 = -i(-i\xi) = -\xi = \alpha_3.$$

So we have shown that $\sigma_4(\alpha_2) = \alpha_1$, $\sigma_4(\alpha_3) = \alpha_2$ and $\sigma_4(\alpha_4) = \alpha_3$. Now we have completed the 5th column. After completing the table, we can identify the Galois group of the extension E/\mathbb{Q} . In the table we have represented the automorphisms of the Galois group G as permutations. So,

$$G = \{(1), (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), (2, 4), (1, 2)(3, 4), (1, 3), (1, 4)(2, 3)\}.$$

In G , we have 5 elements of order 2 and 2 elements of order 4. It is easy to see that G is non-Abelian. But we know that there are exactly 2 non-isomorphic, non-Abelian groups of order 8. One of them is the quaternion group, which has one element of order 2; and the other is the dihedral group, which has 5 elements of order 2. Therefore $G \cong \mathbb{D}_8$. Now, we find all subgroups of G and compute all fixed subfields which correspond to these subgroups. Since G has order 8, it has subgroups of order 1, 2, 4, 8. We have that

$$G_0 = \{(1)\}$$

is the subgroup of G of order 1, and

$$G_1 = \{(1), (2, 4)\}, G_2 = \{(1), (1, 3)\}, G_3 = \{(1), (1, 2)(3, 4)\}$$

$$G_4 = \{(1), (1, 3)(2, 4)\}, G_5 = \{(1), (1, 4)(2, 3)\}$$

are subgroups of G of order 2. Now other subgroups of G which have order 4 can also be determined. They are,

$$G_6 = \{(1), (1, 3), (2, 4), (1, 3)(2, 4)\}, G_7 = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$G_8 = \{(1), (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}.$$

The subgroup of G of order 8 is itself, which we denote by $G_9 = G$. Now we find the corresponding subfields to these subgroups of G . Since $E = \mathbb{Q}(i, \xi) = \mathbb{Q}(i, \sqrt[4]{2})$, we have that E is generated by the 8 elements

$$1, i, \sqrt[4]{2}, \sqrt{2}, \sqrt[3]{2}, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[3]{2}$$

over \mathbb{Q} . So we have that $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i\sqrt{2})$ are some of the intermediate fields of E/\mathbb{Q} . Clearly, they are fixed subfields of some of the above subgroups of G . We don't compute all the fixed subfields of the extension E/\mathbb{Q} . They can be computed in a similar way. Now we compute the fixed subfield of the subgroup

$$G_4 = \{(1), (1, 3)(2, 4)\} = \langle \sigma_3 \rangle$$

of G . Let $x \in E$ be such that $\sigma_3(x) = x$. Then these x 's will be the elements of the fixed subfield of G_4 over \mathbb{Q} . Since $x \in E$ we have

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4i + a_5i\xi + a_6i\xi^2 + a_7i\xi^3$$

for some elements $a_0, a_1, \dots, a_7 \in \mathbb{Q}$. Then,

$$\begin{aligned} \sigma_3(x) &= \sigma_3(a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4i + a_5i\xi + a_6i\xi^2 + a_7i\xi^3) \\ &= a_0 + a_1\sigma_3(\xi) + a_2\sigma_3(\xi^2) + a_3\sigma_3(\xi^3) + a_4\sigma_3(i) + a_5\sigma_3(i)\sigma_3(\xi) \\ &\quad + a_6\sigma_3(i)\sigma_3(\xi^2) + a_7\sigma_3(i)\sigma_3(\xi^3) \\ &= a_0 + a_1(-\xi) + a_2(\xi)^2 + a_3(-\xi^3) + a_4i \\ &\quad + a_5i(-\xi) + a_6i\xi^2 + a_7i(-\xi^3) \\ &= x. \end{aligned}$$

Hence we obtain

$$a_1 = -a_1, a_2 = a_2, a_3 = -a_3, a_4 = a_4, a_5 = -a_5, a_6 = a_6, a_7 = -a_7.$$

But this implies that $a_1 = a_3 = a_5 = a_7 = 0$. So, x can be written as

$$x = a_0 + a_2\xi^2 + a_4i + a_6i\xi^2 = a_0 + a_2\sqrt{2} + a_4i + a_6i\sqrt{2}.$$

Hence the fixed subfield of G_4 over \mathbb{Q} is $\mathbb{Q}(i, \sqrt{2})$. For the other subgroups of G which have order 2, computing the corresponding fixed subfield is similar. Now we list all the subgroups of G together with the fixed subfields of the extension E/\mathbb{Q} corresponding to the subgroups.

The subgroups of G

$$\begin{aligned} G_0 &= \{(1)\} \\ G_1 &= \{(1), (2, 4)\} \\ G_2 &= \{(1), (1, 3)\} \\ G_3 &= \{(1), (1, 2)(3, 4)\} \\ G_4 &= \{(1), (1, 3)(2, 4)\} \\ G_5 &= \{(1), (1, 4)(2, 3)\} \\ G_6 &= \{(1), (1, 3), (2, 4), (1, 3)(2, 4)\} \end{aligned}$$

The corresponding fixed subfields

$$\begin{aligned} F_0 &= \mathbb{Q}(i, \sqrt[4]{2}) = E \\ F_1 &= \mathbb{Q}(\sqrt[4]{2}) \\ F_2 &= \mathbb{Q}(i\sqrt[4]{2}) \\ F_3 &= \mathbb{Q}(\sqrt[4]{2}(1+i)) \\ F_4 &= \mathbb{Q}(i, \sqrt{2}) \\ F_5 &= \mathbb{Q}(\sqrt[4]{2}(1-i)) \\ F_6 &= \mathbb{Q}(\sqrt{2}) \end{aligned}$$

$$\begin{array}{ll}
G_7 = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} & F_7 = \mathbb{Q}(i\sqrt{2}) \\
G_8 = \{(1), (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\} & F_8 = \mathbb{Q}(i) \\
G_9 = \{(1), (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2) \\
(24), (1, 2)(3, 4), (1, 3), (1, 4)(2, 3)\} & F_9 = \mathbb{Q}
\end{array}$$

Using the table we can easily see that the corresponding subgroup of the subfield $\mathbb{Q}(i)$ is G_8 , since all automorphisms in G_8 fix i and \mathbb{Q} . Clearly, we can also see this in the above diagram. Now we check that F_7 is the fixed subfield of G_7 . We show that the automorphisms in G_7 fix $i\sqrt{2} = i\xi^2 = i\xi\xi = \alpha_2\alpha_1$. We have

$$\begin{aligned}
(1, 2)(3, 4)(\alpha_2\alpha_1) &= \sigma_6(\alpha_2)\sigma_6(\alpha_1) = \alpha_1\alpha_2 = \alpha_2\alpha_1. \\
(1, 3)(2, 4)(\alpha_2\alpha_1) &= \sigma_3(\alpha_2)\sigma_3(\alpha_1) = \alpha_4\alpha_3 = (-i\xi)(-\xi) = i\xi^2 = \alpha_2\alpha_1 \\
(1, 4)(2, 3)(\alpha_2\alpha_1) &= \sigma_8(\alpha_2)\sigma_8(\alpha_1) = \alpha_3\alpha_4 = (-\xi)(-i\xi) = \alpha_2\alpha_1.
\end{aligned}$$

Hence we have shown that $i\xi^2$ is fixed by the elements of G_7 . Therefore, the subfield F_7 of E/\mathbb{Q} corresponds to G_7 . We can also check the corresponding subfield F_6 of the subgroup G_6 in a similar way. The fixed subfields of G_0 and G_9 follow immediately from the definition of the Galois group. \square

Example 2.6.14. Consider the polynomial $f = X^3 + X + 1$ over the field

$$F = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}.$$

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f . Then a splitting field of the polynomial f over F is $E = F(\alpha_1, \alpha_2, \alpha_3)$. So the Galois group of f is $\text{Gal}(E/F)$. E/F , being finite, is algebraic. So, E/F is a separable extension, since it is an algebraic extension over a finite field $F = \mathbb{Z}_2$. Clearly, f is irreducible over F . If f were reducible over F , then it would have a root in F . But we have $f(\bar{0}) = \bar{1}$, and $f(\bar{1}) = \bar{1}$. So, f is irreducible over F .

Now we can use the following result which says that:

If $f \in \mathbb{F}_q[X]$ is irreducible of degree n . Then, a splitting field of f is

$$\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(f) = \mathbb{F}_q(\zeta),$$

where $\zeta = \hat{x}$ in $\mathbb{F}_q[X]/(f)$ and the distinct roots of f are

$$\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{n-1}}.$$

Let $\alpha_1 = \zeta$. Then we have $\alpha_2 = \zeta^2$ and $\alpha_3 = \zeta^4$. Since $\zeta^3 = \zeta + 1$, we have that $\zeta^4 = \zeta^3 \cdot \zeta = (\zeta + 1)\zeta = \zeta^2 + \zeta$. Now we have

$$E = F(\alpha_1, \alpha_2, \alpha_3) = F(\zeta).$$

Since $[E : F] = 3$ there are no intermediate fields of the extension E/F . Since f is a separable polynomial over F , and E is a splitting field of f over F , by Proposition 2.6.5 we have that $|\text{Gal}(E/F)| = [E : F]$. So,

$$|\text{Gal}(E/F)| = 3.$$

Thus, $\text{Gal}(E/F) \cong \mathbb{Z}_3$. We also express G such that $\text{Gal}(E/F) = \{(1), (1, 2, 3), (1, 3, 2)\}$. There are two subgroups of the group $\text{Gal}(E/F)$, namely $\{(1)\}$ and itself. Now we can list the subgroups of $\text{Gal}(E/F)$ and the corresponding subfields of E/F . \square

The subgroups of G	The corresponding fixed subfields
$G_0 = \{(1)\}$	$F_0 = E$
$G_1 = \{(1), (1, 2, 3), (1, 3, 2)\}$	$F_1 = F = \mathbb{Z}_2$

\square

Now we can start the last section of the first part. In this section we prove the Galois' Criterion for Solvability by Radicals.

2.7 The Galois' Criterion for Solvability by Radicals

We start this section by defining the concept of solvability of an equation by radicals over a field F . Also we give the definition of a radical extension. Then, we prove some results in order to be able to prove Galois' Criterion for Solvability by Radicals.

Definition 2.7.1. Let $f \in F[X]$ be monic of positive degree. Then the equation $f = 0$ is solvable by radicals over F if there exists a field extension E/F which possesses a tower of subfields

$$F = F_1 \subseteq F_2 \subseteq \dots \subseteq F_{r+1} = E \quad (2.7.1)$$

where each $F_{i+1} = F_i(b_i)$ and $b_i^{n_i} = a_i \in F_i$ and E contains a splitting field over F of f . A tower of subfields such as (2.7.1) is called a root tower of F for E . \square

Since each subfield F_{i+1} of E is obtained by adjoining a root $b_i = \sqrt[n_i]{a_i}$ of the equation $X^{n_i} - a_i = 0$ to the field F_i and all the roots of f are contained in the field E , this definition says that every root of f can be obtained by starting with the elements of the base field and having a finite sequence of rational operations and solving equations of the form $X^n - a = 0$.

Definition 2.7.2. A field extension E/F is said to be a classical radical extension of F , if we have $E = F(u_1, u_2, \dots, u_m)$, where for all u_i , $i \in \{1, 2, \dots, m\}$ there exists some $n_i \in \mathbb{N}^*$ such that $u_i^{n_i} = a \in F(u_1, u_2, \dots, u_{i-1})$. We denote $u_i = \sqrt[n_i]{a}$ and call it as an n_i -th radical of a . \square

Using the second definition, we can say that the extension E/F in the first definition is a classical radical extension.

Let f has distinct roots in a splitting field $E \supseteq F$. We know that the Galois group of the polynomial f is the Galois group of the extension E/F . Let $G = \text{Gal}(E/F)$, and

$$f = (X - r_1)(X - r_2) \dots (X - r_n)$$

in $E[X]$. Then $E = F(r_1, r_2, \dots, r_n)$ since E is a splitting field of f . Let

$$R = \{r_1, r_2, \dots, r_n\}$$

be the set of roots of f .

Now we show that we can also identify the Galois group of the extension E/F with a permutation group of the set R . Actually, Galois defined the Galois group as a permutation group of the set of roots of f . On the other hand, Dedekind realized that

this group can also be defined as the group of F -automorphisms of the splitting field of f . Since we used the Dedekind's definition, now we show that we can also define the Galois group of an extension E/F as a permutation group of the set R .

Let $\eta \in G$. By Lemma 2.6.2, we have $\eta(R) = R$. Hence, η induces a permutation of R . Now there is a homomorphism

$$\zeta : \eta \mapsto \eta|_R$$

of G into the symmetric group S_n of the permutations of the roots of f . Since the roots of f generate E/F we obtain

$$\zeta(\eta) = \eta|_R = 1 \iff \eta|_E = 1,$$

which means that η is the identity automorphism on G . But this shows that the kernel of ζ consists only of the identity automorphism. So, we have that ζ is a monomorphism of G into S_n . Therefore, G is isomorphic to a subgroup of S_n . We denote the image of ζ by G_f . If $G_f = S_n$ then the Galois group of the polynomial f is the symmetric group S_n .

Definition 2.7.3. Let E be an over field of F . E/F is called *Abelian* (resp. *cyclic*) if it is Galois over F and $G = \text{Gal}(E/F)$ is Abelian (resp. cyclic). \square

Before proving our first lemma, we are going to provide a result which is used in the proof of it.

Proposition 2.7.4. Let f be a monic polynomial of positive degree in $F[X]$. Then all the roots of f in any splitting field E/F are simple if and only if $\text{gcd}(f, f') = 1$.

Proof. Let $d = \text{gcd}(f, f')$ in $F[X]$. Suppose that f has a multiple root in $E[X]$. Then we have $f = (X - r_1)^k g(X)$ where $k > 1$. If we take the derivative of both sides, then we obtain

$$f' = k(X - r_1)^{k-1}g + (X - r_1)^k g'.$$

Since $k \geq 2$, clearly $(X - r_1)^k$ divides f' . So, $(X - r_1)^k$ divides both f and f' . This shows that $d \neq 1$.

Conversely, suppose that all roots of f are simple. Then,

$$f = \prod_{i=1}^n (X - r_i)$$

in $E[X]$ and if $i \neq j$ then $r_i \neq r_j$. If we take the derivative of f , we obtain

$$f' = \sum_{i=2}^{n-1} (X - r_1) \dots (X - r_{i-1})(X - r_{i+1}) \dots (X - r_n).$$

This clearly shows that $(X - r_i) \nmid f'$ for all i . Therefore $\gcd(f, f') = 1$. \square

Lemma 2.7.5. *Let E be the splitting field of $f = X^n - 1$ over F of characteristic 0. Then, $G = \text{Gal}(E/F)$ is Abelian, that is, the extension E/F is Abelian.*

Proof. Since the characteristic of F is 0, $f' = (X^n - 1)' = nX^{n-1} \neq 0$. So, we have $\gcd(f, f') = 1$. By Proposition 2.7.4, f has distinct roots in E . Clearly, these roots form a group under multiplication. Also we know that R is cyclic. So, we can write $R = \langle r \rangle$. Then we show that the map

$$\eta \longmapsto \eta|_R$$

of G into $\text{Aut}(R)$ is a monomorphism. Since E is a splitting field of f , the roots of f generate E . If $\eta|_R = 1$, then η is the identity automorphism of E . Hence, the kernel of this map consists only of the identity automorphism. So, this map is a monomorphism. Hence, G is isomorphic to a subgroup of $\text{Aut}(R)$. Now we show that $\text{Aut}(R)$ is an Abelian group. Let $\sigma, \tau \in \text{Aut}(R)$. It is clear that $\text{Aut}(R) \subseteq G$. By Lemma 2.6.2, for $r \in R$, we have $\sigma(r) = r^i$ and $\tau(r) = r^j$, for some $i, j \in \{1, 2, \dots, n\}$. Then,

$$(\sigma\tau)(r) = \sigma(\tau(r)) = \sigma(r^j) = (r^j)^i = r^{ji} = r^{ij} = (r^i)^j = \tau(r^i) = \tau(\sigma(r)) = (\tau\sigma)(r).$$

So, $\text{Aut}(R)$ is an Abelian group since r generates R . Therefore G is also an Abelian group. \square

Lemma 2.7.6. *If F contains n distinct n -th roots of unity, then the Galois group of $X^n - a$ over F is cyclic of order a divisor of n .*

Proof. Let R be the set of n -th roots of unity in F . Let E be the splitting field of the polynomial $X^n - a$. If r is a root of $X^n - a$, then the other roots of this polynomial are

$$r, r\epsilon, r\epsilon^2, \dots, r\epsilon^{n-1},$$

where ϵ is the n -th root of unity in F . Since E is a splitting field of the polynomial $X^n - a$ and $\epsilon \in F$, we have $E = F(r)$. Let $\eta \in G$. Then by Lemma 2.6.2, we have $\eta(r) = r\epsilon^i$, for some i . Now the map

$$\eta \longmapsto \epsilon^i$$

is clearly a monomorphism of G into R . Thus, G is isomorphic to a subgroup of R which is a cyclic group. Hence G is also a cyclic group. Since the order of R is n and G is isomorphic to a subgroup of R , the order of G is a divisor of n . \square

Now we are going to prove Hilbert's Theorem 90. But firstly, we define *trace* and *norm* of an element in a field extension.

Definition 2.7.7. Let E/F be a finite Galois extension with Galois group G such that $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$. For $a \in E$ the trace of a and the norm of a are defined respectively,

$$T(a) = \sigma_1(a) + \sigma_2(a) + \dots + \sigma_n(a)$$

$$N(a) = \sigma_1(a) \cdot \sigma_2(a) \dots \sigma_n(a)$$

Clearly, for $\sigma_i \in G$, $\sigma_i(T(a)) = (\sum_{j=1}^n \sigma_i(\sigma_j(a))) = T(a)$, since $\{\sigma_i\sigma_j \mid 1 \leq j \leq n\}$ is a permutation of $\sigma_1, \sigma_2, \dots, \sigma_n$. So, $T(a) \in F$, and similarly $N(a) \in F$. Now we list some of the preliminary properties of the norm.

- (1) $N(a \cdot b) = N(a) \cdot N(b)$ where $a, b \in E$, that is, the norm function is multiplicative.
- (2) If $\sigma \in G$ and $a \in E$ then $N(\sigma(a)) = N(a)$.

We can also define the norm and trace of an element in a finite, separable extension E/F with degree n . We take $\sigma_1, \sigma_2, \dots, \sigma_n$ as all distinct F -homomorphisms of E into \overline{F} . \square

Theorem 2.7.8. (Hilbert's Theorem 90) Let E/F be a finite, Galois extension where $G = \text{Gal}(E/F)$ is cyclic of order n ; let σ be a generator of G . then $N(a) = 1$ if and only if there exists $b \in E$, $b \neq 0$ such that $a = b\sigma(b)^{-1}$.

Proof. Since σ generates G , we have $N(a) = a\sigma(a)\sigma^2(a)\dots\sigma^{n-1}(a)$. Suppose that

$$a = b\sigma(b)^{-1}.$$

Now we have,

$$N(a) = N(b\sigma(b)^{-1}) = N(b)N(\sigma(b)^{-1}) = N(b)N(\sigma(b))^{-1} = N(b)N(b)^{-1} = 1.$$

Suppose that $N(a) = 1$, and $c \in E$. We define the "partial norms":

$$\begin{aligned} d_0 &= ac, \quad d_1 = a\sigma(a)\sigma(c), \quad d_2 = a\sigma(a)\sigma^2(a)\sigma^2(c), \dots \\ d_{n-1} &= a\sigma(a)\dots\sigma^{n-1}(a)\sigma^{n-1}(c) = \sigma^{n-1}(c), \quad \text{since } N(a) = 1. \\ a\sigma(d_i) &= a\sigma(a)\sigma^2(a)\dots\sigma^{i+1}(a)\sigma^{i+1}(c) = d_{i+1}, \quad \text{for all } 0 \leq i \leq n-2. \end{aligned} \quad (2.7.2)$$

By Dedekind's Lemma⁶, $\{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ is linearly independent over E . So, there exists $c_0 \in G$ such that

$$d_0 + d_1 + \dots + d_{n-1} \neq 0.$$

Now for $c_0 \in G$, let $b = d_0 + d_1 + \dots + d_{n-1}$. We claim that

$$a = b\sigma(b)^{-1}.$$

Now by Equation (2.7.2), we have

$$\sigma(b) = \sigma(d_0) + \sigma(d_1) + \dots + \sigma(d_{n-1}) = a^{-1}[d_1 + d_2 + \dots + d_{n-1}] + \sigma^n(c_0).$$

But $\sigma^n = 1$. Then, $\sigma^n(c_0) = c_0$ and $c_0 = a^{-1}d_0$. Now if we put c_0 in the above equation, we obtain

$$\sigma(b) = a^{-1}[d_0 + d_1 + d_2 + \dots + d_{n-1}].$$

But this implies that $\sigma(b) = a^{-1}b$. Therefore, $a = b\sigma(b)^{-1}$. □

⁶Dedekind's Lemma says: Any set of distinct automorphisms of E is linearly independent over E .

Now we are ready to prove our next lemma.

Lemma 2.7.9. *Let p be prime and assume F contains p distinct p -th roots of unity. Let E/F be cyclic and p dimensional. Then $E = F(b)$ where $b^p \in F$.*

Proof. Let w be a primitive p -th root of unity. Since E/F is cyclic, it is Galois over F and its Galois group is cyclic of order p . Since $w \in F$,

$$N(w) = w^p = 1.$$

We have

$$|G| = |\text{Gal}(E/F)| = [E : F].$$

Let σ be a generator of the cyclic group G . By Hilbert's Theorem 90, $w = b\sigma(b)^{-1}$ for some $b \in E$. Then, $\sigma(b) = w^{-1}b$. So we have,

$$\sigma(b^p) = (w^{-1}b)^p = b^p.$$

Since E/F is a Galois extension and σ generates G , we have $b^p \in \text{Fix}(G) = F$. We also have $b \notin F$, since otherwise, $\sigma(b) = b$ which implies that $w = 1$. But w is a primitive p -th root of unity. So, $F(b) \neq F$. Hence, $F(b)$ is an intermediate field of the extension E/F and it is not equal to F . But E/F is of degree p , where p is a prime number. So, we have $E = F(b)$. \square

Lemma 2.7.10. *Let $f \in F[X]$ and let E be an extension field of F . Then the Galois group of f over E is isomorphic to a subgroup of the Galois group of f over F .*

Proof. Let L be a splitting field of f over E . Since $E \supseteq F$, E contains a splitting field K of f over F by Theorem 2.5.2. If

$$f = \prod_1^n (X - r_i)$$

in $L[X]$, then we can write $L = E(r_1, r_2, \dots, r_n)$. Also $K = F(r_1, r_2, \dots, r_n)$. If

$$\eta \in \text{Gal}(L/E),$$

then η permutes the roots $\{r_1, r_2, \dots, r_n\}$ and η fixes E . Since $F \subseteq E$, η also fixes F . Hence,

$$\eta|_K \in \text{Gal}(K/F).$$

Now we show that the restriction homomorphism, $\eta \mapsto \eta|_K$ of $\text{Gal}(L/E)$ into $\text{Gal}(K/F)$, is a monomorphism. We know that $\eta|_K = 1$ implies that η is identity on L , since L is generated over E by the roots of f . So, this restriction homomorphism is a monomorphism of $\text{Gal}(L/E)$ into $\text{Gal}(K/F)$. Hence, $\text{Gal}(L/E)$ is isomorphic to a subgroup of $\text{Gal}(K/F)$. \square

Let E be a finite dimensional extension field of F of characteristic 0. Then clearly E is algebraic over F . So, there exists a normal closure \tilde{E}/F of the extension E/F , which is also finite dimensional. Let

$$G = \text{Gal}(\tilde{E}/F).$$

Now our aim is to show that \tilde{E} is generated over F by $\eta(E)$ where $\eta \in G$. We call $\eta(E)$ as the *conjugates* of E/F in \tilde{E} . Let \tilde{E}' be the subfield of \tilde{E} which is generated by the $\eta(E)$, $\eta \in G$. Then clearly G maps the subfield \tilde{E}' onto itself. Now we obtain a finite set of automorphisms whose fixed subfield is F , since \tilde{E} is normal and separable over F . But this shows that \tilde{E}' is normal over F by Proposition 2.6.7. But \tilde{E}/F is the normal closure of the extension E/F , which means that it is the “least” normal extension containing E/F as a subextension. Hence, $\tilde{E}' = \tilde{E}$.

Now we are going to prove our last lemma before the Galois’ Criterion for Solvability by Radicals.

Lemma 2.7.11. *Let E/F have a root tower over F , say $F = F_1 \subseteq F_2 \subseteq \dots \subseteq F_{r+1}$ with $F_{i+1} = F_i(b_i)$, $b_i^{n_i} \in F_i$, and assume E is generated over F by a finite set of elements whose minimal polynomials are separable. Then the normal closure \tilde{E}/F of E/F has a root tower over F such that the distinct integers n_i for this tower are the same as those occurring in the given tower.*

Proof. Since E/F is finite, it is algebraic. So, there exists a normal closure \tilde{E}/F of the extension E/F . If we apply $\eta \in \text{Gal}(\tilde{E}/F)$ to the tower of fields

$$F = F_1 \subseteq F_2 \subseteq \dots \subseteq F_{r+1},$$

with $F_{i+1} = F_i(b_i)$, $b_i^{n_i} \in F_i$, then we also have a root tower for $\eta(E)$ over F , since $\eta(F) = F$. Let $\text{Gal}(\tilde{E}/F) = \{\eta_1, \eta_2, \dots\}$. Since $E = F(b_1, b_2, \dots, b_r)$ and we know that the normal closure \tilde{E}/F of E/F is generated by the conjugate fields, $\eta(E)$, $\eta \in \text{Gal}(\tilde{E}/F)$, we have

$$\tilde{E} = F(\eta_1(b_1), \dots, \eta_1(b_r); \eta_2(b_1), \dots, \eta_2(b_r); \dots),$$

By induction on $n_i \in \mathbb{N}^*$, for some $i \in \{1, 2, \dots, r\}$, we can show that the same n_i for all $i \in \{1, 2, \dots, r\}$ will also occur in this root tower. Thus, the normal closure \tilde{E}/F has a root tower over F , with the same n_i 's. \square

Now we can prove the Galois' Criterion for Solvability by Radicals.

Theorem 2.7.12. (*Galois' Criterion for Solvability by Radicals*) *An equation $f = 0$ is solvable by radicals over a field F of characteristic 0 if and only if its Galois group is solvable.*

Proof. Suppose that $f = 0$ is solvable by radicals over F of characteristic 0. Then there exists an extension field \tilde{E}/F containing a splitting field E/F of f , which has a root tower over F as in Equation (2.7.1). Using Lemma 2.7.11, we may assume that \tilde{E}/F is a normal extension. Since E/F is finite, it is algebraic. But we know that any algebraic extension of a field of characteristic 0 is separable, so \tilde{E}/F is a separable extension. Hence, \tilde{E} , being separable and normal over F , is Galois over F .

If n is the least common multiple of the integers n_i , in the root tower of \tilde{E}/F , then we can extend this tower from \tilde{E} to $\tilde{E}(t)$, where t is a primitive n -th root of unity. If \tilde{E} is a splitting field of some polynomial g over F , then g is separable by Proposition 2.6.7. Also $\tilde{E}(t)$ is a splitting field over F of the polynomial $g \cdot (X^n - 1)$, which is clearly separable. Hence, $\tilde{E}(t)$ is separable and normal over F . By Proposition 2.6.7, it is

Galois over F . Since $t^n = 1$ and $1 \in F$, we can rearrange the tower, where we have $F(t)$ as the second term. Then, we obtain

$$F = F_1 \subseteq F_2 = F(t) \subseteq F_3 \subseteq \dots \subseteq \tilde{E}(t). \quad (2.7.3)$$

Let G be the Galois group of the extension E/F , and H be the Galois group of the extension \tilde{E}/F . Using Lemma 2.7.5, we have that F_2 is Abelian over F_1 . Using Lemma 2.7.6, we have that F_{i+1} is Abelian over F_i , for $i > 1$. Since $F_i \supseteq F(t)$, we have that F_i contains n distinct n -th roots of unity. Let H_i be the subgroup of the group $H = \text{Gal}(\tilde{E}(t)/F)$, which corresponds to the subfield F_i . Then we have $H_i = \text{Gal}(\tilde{E}(t)/F_i)$. Since the minimal polynomial of each element of F_{i+1} splits over F_{i+1} for all i , by the definition of the root tower, we have that F_{i+1} is normal over F_i for all i .

By Theorem 2.6.10, we can say that $H_{i+1} \triangleleft G$ for all i . Also we have $H_{i+1} \triangleleft H_i$ for all i . Moreover, by Theorem 2.6.10, we obtain

$$H_i/H_{i+1} \cong \text{Gal}(F_{i+1}/F_i).$$

Hence, H_i/H_{i+1} is an Abelian group, since F_{i+1} is Abelian over F_i for all i . Thus, we have a normal series for H with Abelian factors, so H is solvable. Again by Theorem 2.6.10, we have

$$G = \text{Gal}(E/F) \cong H/\text{Gal}(E/E).$$

We know that E is normal over F . Hence G is solvable from Proposition 2.2.5, since it is isomorphic to a quotient group of H .

Conversely, assume that the Galois group G of f is solvable. Let E be a splitting field of the polynomial f over F . Then $\text{Gal}(E/F) = G$. Clearly, E/F is an algebraic extension of a field of characteristic 0. Then E/F is a separable extension. This says that f is separable over F , since all its irreducible factors are separable in $F[X]$. So, by Proposition 2.6.5, we have $|G| = [E : F]$. Let $n = |G| = [E : F]$. We put

$$F_1 = F, \quad F_2 = F(t),$$

where t is a primitive n -th root of unity and $\tilde{E} = E(t)$. By Lemma 2.7.10, we have that the Galois group of f over F_2 , which is the Galois group of \tilde{E}/F_2 , is isomorphic to a subgroup H of G . By Proposition 2.2.4, H , being a subset of G , is also solvable. By Proposition 2.2.3, H has a normal series such that

$$1 = H_{r+1} \triangleleft \dots \triangleleft H_2 \triangleleft H_1 = H,$$

with factors H_i/H_{i+1} cyclic of prime order p_i , for all $1 \leq i \leq r$.

Correspondingly, we have an increasing chain of subfields such that

$$F_2 \subseteq F_3 \subseteq \dots \subseteq F_{r+2} = \tilde{E}.$$

We have, $H_i = \text{Gal}(\tilde{E}/F_{i+1})$. By Proposition 2.7.10, we have that F_{i+1} is normal over F_i , and H_i/H_{i+1} is isomorphic to the Galois group of F_{i+1}/F_i . Hence, F_{i+1}/F_i has a cyclic Galois group with prime order p_i for all i . Since $\text{Gal}(F_{i+1}/F_i)$ is a subgroup of G , we have $p_i \mid |G|$. But $F_i \supseteq F_2$, so F_i contains a primitive n -th root of unity. Since $p_i \mid |G|$, F_i contains p_i distinct p_i -th roots of unity. By Lemma 2.7.9, we have $F_{i+1} = F_i(b_i)$, where $b_i^{p_i} \in F_i$. Hence, \tilde{E} possesses a root tower over F , where \tilde{E} contains a splitting field over F of the polynomial f . Therefore, $f = 0$ is solvable by radicals over F . \square

Now we give an example of an insoluble quintic polynomial. We claim that the polynomial $f = X^5 - 6X + 3$ is not solvable by radicals over \mathbb{Q} . In order to do that, we have to give a result first.

Theorem 2.7.13. *Let p be prime number, and let f be an irreducible polynomial of degree p over \mathbb{Q} . Suppose that f has exactly two non-real roots in \mathbb{C} . Then the Galois group of f over \mathbb{Q} is S_p .*

Proof. By the Fundamental Theorem of Algebra, we know that \mathbb{C} contains a splitting field of the polynomial f . Let $E \subseteq \mathbb{C}$ be a splitting field of the polynomial f . Then the Galois group of f is $G = \text{Gal}(E/\mathbb{Q})$. Since E is an algebraic extension over a field of characteristic 0, E/\mathbb{Q} is a separable extension. So, all roots of f are distinct. Then,

G is isomorphic to a subgroup of S_p . Also, $|G| = [E : \mathbb{Q}]$. Let $u \in E \setminus \mathbb{Q}$ be a root of f . Then,

$$[\mathbb{Q}(u) : \mathbb{Q}] = p,$$

since f is an irreducible polynomial over \mathbb{Q} of degree p . Then, $p \mid [E : \mathbb{Q}]$, but we have $|G| = [E : \mathbb{Q}]$. So, we obtain $p \mid |G|$.

By Cauchy's Lemma (it will be discussed in the following chapter in Lemma 4.4.19), G contains an element of order p . This implies that G contains a p -cycle, since the only elements of S_p of order p are the p -cycles. Also we know that the complex conjugation (sends two non-real roots to each other and leaves the other real roots fixed) induces an automorphism of E , fixing \mathbb{Q} pointwise. But complex conjugation is a transposition. Therefore without loss of generality, we may assume that G contains $(1, 2)$ and $(1, 2, 3, \dots, p)$.

We claim that these two permutations generate S_p . Let H be a subgroup of G that is generated by these permutations. We put

$$b = (1, 2) \text{ and } c = (1, 2, 3, \dots, p).$$

Then, $cbc^{-1} = (2, 3) \in H$ and $c(2, 3)c^{-1} = (3, 4) \in H$. Suppose that for some $i < p$, $(i, i+1) \in H$. Then, $c(i, i+1)c^{-1} = (i+1, i+2) \in H$. So by induction on i , all transpositions of the form $(i, i+1)$ lies in H . Also

$$(1, 2)(2, 3)(1, 2) = (1, 3) \in H, \quad (1, 3)(3, 4)(1, 3) = (1, 4) \in H.$$

Now suppose for some $i < p$, we have that $(1, i)$ lies in H . Then,

$$(1, i)(i, i+1)(1, i) = (1, i+1) \in H.$$

Hence, by induction on i , we have that S_p contains all transpositions of the form $(1, i)$. Let $i, j \in \{1, 2, \dots, p\}$ and $i \neq 1 \neq j$. Then,

$$(i, j) = (1, i)(1, j)(1, i) = (i, j) \in H.$$

But we know that any permutation in S_p can be written as a product of transpositions, so $H = S_p$. Hence S_p is generated by $(1, 2)$ and $(1, 2, 3, \dots, p)$. Since we have shown that $H = S_p \leq G$, we have $G = S_p$. \square

Now we aim to say that the Galois group of the polynomial $f = X^5 - 6X + 3$ is S_5 , by using Theorem 2.7.12. By Eisenstein's Criterion, we know that f is irreducible over \mathbb{Q} . Now we show that f has exactly three real roots, so we are able to say that f has exactly two non-real roots, since f is a separable polynomial over \mathbb{Q} . Firstly, we evaluate f at

$$x = -2, -1, 0, 1, 2$$

to see the behavior of f around 0. $f(-2) = -17$, $f(-1) = 8$, $f(0) = 3$, $f(1) = -2$, $f(2) = 23$. This shows that f passes the x -axis at least three times, since f is a continuous function defined on \mathbb{R} . Since f can not change sign without passing through the x -axis, f has at least three real roots.

Rolle's Theorem says that if t_1 and t_2 are two roots of f then there exists $c \in (t_1, t_2)$ such that $f'(c) = 0$. But $f' = 5X^4 - 6$ has only two roots which are $\pm\sqrt[4]{6/5}$. So, f has at most three real roots. Hence, f has exactly three real roots and two non-real roots. Now we can use Theorem 2.7.13.

Now that $f = X^5 - 6X + 3$ satisfies the conditions of the polynomial given in the Theorem 2.7.13, the Galois group of the polynomial f is S_5 . But we know that S_5 is not a solvable group. Therefore, $f = X^5 - 6X + 3$ over \mathbb{Q} is not solvable by radicals by Theorem 2.7.12.

Chapter 3

COGALOIS THEORY

In this chapter we investigate Cogalois Theory. We start by providing some results which will be used in the proof of The Vahlen-Capelli Criterion. This is a criterion which deals with the irreducibility of binomials $X^n - a$ over an arbitrary field. Then we define some concepts such as G -radical extensions and G -Kneser extensions which are used in defining Cogalois and G -Cogalois extensions. We also define Galois and Cogalois connections and strongly G -Kneser extensions. Then the definition of G -Cogalois extensions will be given. Lastly, we present some examples of G -Cogalois extensions.

3.1 The Vahlen-Capelli Criterion

Lemma 3.1.1. *Let $a \in F$, and let $m, n \in \mathbb{N}^*$ be relatively prime. Then, the polynomial $X^{mn} - a$ is irreducible in $F[X]$ if and only if polynomials $X^m - a$ and $X^n - a$ are both irreducible in $F[X]$.*

Proof. We can write $X^{mn} - a = (X^n)^m - a = (X^m)^n - a$. Suppose that $X^{mn} - a$ is irreducible and $X^n - a$ or $X^m - a$ is reducible in $F[X]$. If $X^n - a$ is reducible over F , then we have

$$X^n - a = f \cdot g,$$

where $f, g \in F[X]$ and $\deg(f), \deg(g) < n$. If we replace X by X^m , then we obtain

$$X^{mn} - a = f(X^m)g(X^m)$$

in $F[X]$, where $\deg(f(X^m)), \deg(g(X^m)) < mn$. But this shows that $X^{mn} - a$ is reducible over F , which is a contradiction. Similarly, assuming that $X^m - a$ is reducible

over F , we again obtain a contradiction. Hence, if $X^{mn} - a$ is irreducible in $F[X]$, then both of the polynomials $X^n - a$ and $X^m - a$ should be irreducible in $F[X]$.

Conversely, assume that both of the polynomials $X^n - a$ and $X^m - a$ are irreducible in $F[X]$. Now let $u \in \Omega$ be a root of the polynomial $X^{mn} - a$. Then $u^{mn} - a = 0$. So, we can see that $(u^m)^n - a = 0$. Hence, u^m is a root of the polynomial $X^n - a$ which is assumed to be irreducible. Similarly, u^n is a root of the irreducible polynomial $X^m - a$. Hence we have,

$$[F(u^m) : F] = n \text{ and } [F(u^n) : F] = m.$$

But we know that

$$F \subseteq F(u^m) \subseteq F(u) \text{ and } F \subseteq F(u^n) \subseteq F(u),$$

so, we can say that $[F(u^m) : F] = n \mid [F(u) : F]$ and $[F(u^n) : F] = m \mid [F(u) : F]$. Hence $\text{lcm}(m, n) = mn \mid [F(u) : F]$, since m and n are relatively prime. So we have $mn \leq [F(u) : F]$. But u is assumed to be a root of the polynomial $X^{mn} - a$, so

$$[F(u) : F] \leq mn.$$

Therefore, we obtain $[F(u) : F] = mn$, which means that $\text{Min}(u, F) = X^{mn} - a$. In other words, $X^{mn} - a$ is irreducible in $F[X]$. \square

Lemma 3.1.2. *Let $p \in \mathbb{P}$ and $a \in F$. Then $X^p - a$ is irreducible in $F[X]$ if and only if $a \notin F^p$.*

Proof. Suppose that $a \in F^p$. Then we have $a = b^p$, for some $b \in F$. So, $X^p - a = X^p - b^p$ is reducible in $F[X]$, since $X - b \in F[X]$ is a factor of $X^p - a$.

Conversely, assume that $a \notin F^p$. Suppose that $X^p - a$ is reducible in $F[X]$. Let f be an irreducible factor of degree n of $X^p - a$. Then $1 \leq n < p$.

Let $u \in \Omega$ be a root of f . So the roots of f in Ω are of the form $\zeta^i u$, $0 \leq i \leq p-1$, where $\zeta \in \Omega$ is a p -th root of unity. Let $c = f(0)$, so we have that $\pm c$ is the product of the roots of f . We have $\pm c = u \cdot \zeta u \cdot \zeta^2 u \cdots \zeta^{n-1} u = \zeta^{n(n-1)/2} u^n$.

Now we put $\zeta^{n(n-1)/2} = \xi$, where $\xi \in \Omega$ is a p -th root of unity. Then, $\pm c = \xi u^n$. Since $n < p$ and p is prime, n and p are relatively prime integers. So, there exists some integers r, s such that $rn + sp = 1$. Now we obtain

$$u = u^{rn+sp} = (u^n)^r (u^p)^s = (\pm c \xi^{-1})^r a^s.$$

Thus, $u \xi^r = (\pm c)^r a^s$. Since $X^p - a$ is assumed to be reducible in $F[X]$, we have $a^s, c^r \in F$. Hence, $u \xi^r \in F$. But $a = u^p = u^p (\xi^r)^p = (u \xi^r)^p \in F^p$ leads to a contradiction. \square

Lemma 3.1.3. *Let $p \in \mathbb{P}$ and $a \in F$ be such that $X^p - a$ reducible in $F[X]$ and let $u \in \Omega$ be a root of $f = X^p - a$. Then the following statements hold.*

(1) *If $p > 2$, or if $p = 2$ and $\text{Char}(F) = 2$, then $u \notin F(u)^p$.*

(2) *If $p = 2$ and $\text{Char}(F) \neq 2$, then $u \in F(u)^2$ if and only if $-4a \in F^4$.*

Proof. (1) Suppose that $u \in F(u)^p$. Then, we have $u = v^p$, for some $v \in F(u)$. Since $u \in \Omega$ is a root of the irreducible polynomial f , we have $[F(u) : F] = p$. We can write $v = \sum_{k=0}^{p-1} c_k u^k$, where $c_0, c_1, \dots, c_{p-1} \in F$. If $\text{Char}(F) = p$, then

$$u = v^p = \left(\sum_{k=0}^{p-1} c_k u^k \right)^p = \sum_{k=0}^{p-1} c_k^p (u^p)^k = \sum_{k=0}^{p-1} c_k^p a^k.$$

But $\sum_{k=0}^{p-1} c_k^p a^k \in F$, since every term in this sum is in F . Hence, $u \in F$. So, we have $a = u^p \in F^p$. But this contradicts Lemma 3.1.2, since f is irreducible by hypothesis. In particular, $u \notin F(u)^p$, for $p = 2 = \text{Char}(F)$.

Suppose that $\text{Char}(F) \neq p$ and $u \in F(u)^p$. Now we put $u = v^p$, for some $v \in F(u)$. Consider the field $E = F(u, \zeta_p)$, where ζ_p is a primitive p -th root of unity. Clearly, E is a splitting field of the polynomial $f \in F[X]$.

This polynomial is separable, since it has distinct roots in any splitting field of f . Hence E/F is a normal extension by Proposition 2.6.7. So, any $\sigma \in \text{Gal}(E/F)$ sends u into some other root of f .

On the other hand, we know that for every $0 \leq i \leq p-1$, $u \zeta_p^i$ is a root of the irreducible polynomial f . So, the minimal polynomials of these roots over F are the same, that is $X^p - a$.

Hence all of these roots are conjugates elements of each other over F . Thus, for $u\zeta_p^i$, there exists $\sigma_i \in \text{Gal}(E/F)$ such that $\sigma_i(u) = u\zeta_p^i$. Now we put $v_i = \sigma_i(v)$, where $0 \leq i \leq p-1$. Since $u = v^p$, we have

$$\sigma_i(u) = \sigma_i(v^p) = (\sigma_i(v))^p = v_i^p.$$

By Lemma 3.1.2, we can see that $a \notin F^p$, which means that $u^p \notin F^p$. This implies that $u \notin F$, but $u = v^p$ so we have, $v \in F(u) \setminus F$. Hence, $F(v) \subseteq F(u)$. On the other hand, we also have $F(u) = F(v^p) \subseteq F(v)$. Thus, $F(u) = F(v)$. If we put $f := \text{Min}(v, F)$, then

$$\deg(f) = [F(v) : F] = [F(u) : F] = \deg(X^p - a) = p.$$

Now for every $i, j \in \{0, 1, \dots, p-1\}$, $\sigma_i(u) \neq \sigma_j(u)$ holds. Since otherwise we have, $\zeta_p^{i-j} = 1$, but $i-j < p$ and order of ζ_p is p in Ω^* . Hence, for every $i, j \in \{0, 1, \dots, p-1\}$, we observe that $\sigma_i(u) \neq \sigma_j(u)$. Also $\sigma_i(v) \neq \sigma_j(v)$, for all $i, j \in \{0, 1, \dots, p-1\}$, since $u = v^p$. Because, $\sigma_i \in \text{Gal}(E/F)$, for all $i \in \{0, 1, \dots, p-1\}$, we have that σ_i fixes the elements of F pointwise. So for all $i \in \{0, 1, \dots, p-1\}$, we obtain $f(\sigma_i(v)) = \sigma_i(f(v)) = 0$, since v is a root of f . This implies that f has at least p distinct roots in Ω , which are v_0, v_1, \dots, v_{p-1} . But the degree of f is p , so v_0, v_1, \dots, v_{p-1} are exactly all the roots of f in Ω . Since f is a polynomial over F , the product of the roots of f , say $w = \prod_{k=0}^{p-1} v_k \in F$. Now, if we multiply the equalities $\zeta_p^k u = v_k^p$, $k = 0, 1, \dots, p-1$, then we obtain

$$\prod_{k=0}^{p-1} \zeta_p^k u = \prod_{k=0}^{p-1} v_k^p = \left(\prod_{k=0}^{p-1} v_k \right)^p = w^p.$$

Now we put

$$\eta = \prod_{k=0}^{p-1} \zeta_p^k = \zeta_p^{p(p-1)/2},$$

and we obtain $\eta u^p = \eta a = w^p$.

If $p > 2$, then $(p-1)/2 \in \mathbb{Z}$. And this implies that $\eta = 1$, since the order of ζ_p is p . So we obtain $a = w^p \in F^p$. But this leads to a contradiction, since $X^p - a$ is

irreducible over F , and according to the Lemma 3.1.2, a should not be an element of F^p . Hence we have proven (1).

(2) Let $p = 2$ and $\text{Char}(F) \neq 2$. Suppose that $u \in F(u)^2$. Then $u = v^2$, where $v = \alpha + \beta u$, $\alpha, \beta \in F$. Now we have

$$u = v^2 = (\alpha + \beta u)^2 = \alpha^2 + \beta^2 u^2 + 2\alpha\beta u = \alpha^2 + \beta^2 a + 2\alpha\beta u.$$

Since $\{1, u\}$ is a basis of the vector space $F(u)$ over F , we have

$$\alpha^2 + \beta^2 a = 0 \text{ and } 2\alpha\beta = 1.$$

If we write $\beta = 1/2\alpha$, then we obtain $\alpha^2 + (1/4\alpha^2)a = 0$. Thus, $a = -4\alpha^4$. So we have,

$$-4a = 16\alpha^4 = (2\alpha)^4 \in F^4,$$

since $\alpha \in F$.

Conversely, suppose that $-4a \in F^4$. Since $\text{Char}(F) \neq 2$, there exists $\gamma \in F^*$ such that $-4a = \gamma^4$. We have $4 \mid -4a$ so, $2 \mid \gamma^4$. Now we have $-4a = \gamma^4 = (2\alpha)^4$, where $\alpha \in F^*$. Then, $-a = -u^2 = 4\alpha^4$. But this implies that $4\alpha^4 + u^2 = 0$. If we take $\beta = (2\alpha)^{-1} \in F^*$, then clearly,

$$(\alpha + \beta u)^2 = \alpha^2 + \beta^2 u^2 + 2\alpha\beta u = u.$$

Therefore $u = (\alpha + \beta u)^2 \in F(u)^2$. Hence we have proven (2). \square

Lemma 3.1.4. *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$, $n \geq 2$, and $a \in F$.*

- (1) *If $p > 2$, or if $p = 2$ and $\text{Char}(F) = 2$, then $X^{p^n} - a$ is irreducible in $F[X]$ if and only if $a \notin F^p$.*
- (2) *If $p = 2$ and $\text{Char}(F) \neq 2$, then $X^{2^n} - a$ is irreducible in $F[X]$ if and only if $a \notin F^2$ and $-4a \notin F^4$.*

Proof. (1) Suppose that $a \in F^p$. Then $a = b^p$ for some $b \in F$. So, we have

$$X^{p^n} - a = (X^{p^{n-1}})^p - b^p.$$

But this polynomial is divisible by $X^{p^{n-1}} - b$.

Conversely, suppose that $a \notin F^p$. Let $v \in \Omega$ be a root of $X^{p^n} - a$. We put $u := v^{p^{n-1}}$, so we obtain $u^p = (v^{p^{n-1}})^p = v^{p^n} = a$. Consider the polynomial $X^p - a$. Now we have that $u \in \Omega$ is a root of this polynomial. But $a \notin F^p$. So, by Lemma 3.1.2, we have that $X^p - a$ is irreducible in $F[X]$. Hence, $[F(u) : F] = p$, since the minimal polynomial of u over F is $X^p - a$.

Clearly $X^{p^n} - a$ is irreducible in $F[X]$ if and only if the minimal polynomial of v over F is $X^{p^n} - a$, in other words v has degree p^n over F .

Now we prove by induction on n that $X^{p^n} - a$ is irreducible over F . For $n = 1$, $X^p - a$ is irreducible in $F[X]$ by Lemma 3.1.2. So, v has degree p over F . From Lemma 3.1.3 (1), we can say that $u \notin F(u)^p$. So, the polynomial $X^{p^{n-1}} - u \in F(u)[X]$ is irreducible over $F(u)$ by induction hypothesis. We have defined u such that $u := v^{p^{n-1}}$, so v is a root of this irreducible polynomial. Hence, the degree of v over $F(u)$ is p^{n-1} . Consequently, the degree of v over F is p^n , since v has degree p over F . This proves that $X^{p^n} - a$ is irreducible over F . Hence we have proven (1).

(2) Now let $p = 2$ and $\text{Char}(F) \neq 2$. Also assume that $a \in F^2$ or $-4a \in F^4$. If $a \in F^2$, then $a = b^2$ for some $b \in F$. Then, $X^{2^n} - a = (X^{2^{n-1}})^2 - b^2$. But this implies that $X^{2^{n-1}} - b$ divides $X^{2^n} - a$. Therefore, $X^{2^n} - a$ is reducible in $F[X]$. Now assume that $-4a \in F^4$. Then, $-4a = c^4$ for some $c \in F$. Since $\text{Char}(F) \neq 2$, we have $c = 2b$ for some $b \in F^*$. Hence we obtain

$$a = -4^{-1}c^4 = -4^{-1}2^4b^4 = -4b^4.$$

Now we put $Y := X^{2^{n-2}}$. Then

$$\begin{aligned} X^{2^n} - a &= Y^4 + 4b^4 = Y^4 + 4b^2Y^2 + 4b^4 - 4b^2Y^2 \\ &= (Y^2 + 2b^2)^2 - (2bY)^2 = (Y^2 + 2bY + 2b^2)(Y^2 - 2bY + 2b^2). \end{aligned}$$

This shows that $X^{2^n} - a$ is reducible in $F[X]$, since $b \in F$.

Conversely, assume that $\text{Char}(F) \neq 2$, $a \notin F^2$ and $-4a \notin F^4$. We have to prove that $X^{2^n} - a$ is irreducible over F . We do induction on n . Let $v \in \Omega$ be a root of $X^{2^n} - a$. Then we put $u = v^{2^{n-1}}$. Clearly, $u^2 = a$. Consider the polynomial $X^2 - a$.

We can see that u is a root of this polynomial. Since $a \notin F^2$, by Lemma 3.1.2, $X^2 - a$ is irreducible over F . Hence, the minimal polynomial of u over F is $X^2 - a$. Thus, $[F(u) : F] = 2$. In the proof of (1), the fact that $X^{2^n} - a$ is irreducible over F means exactly that $X^{2^{n-1}} - u$ is irreducible over $F(u)$.

We know that for $n = 2$, u is a root of $X^2 - a$, and $X^2 - a$ is irreducible over F . We also assumed that $-4a \notin F^4$. Now we can use Lemma 3.1.3 (2), and obtain $u = v^2 \notin F(u)^2$. So, $X^2 - u$ is irreducible over $F(u)$ by Lemma 3.1.2.

If $n > 2$, then by the induction hypothesis, $X^{2^{n-1}} - u \in F(u)[X]$ is irreducible over $F(u)$ if and only if $u \notin F(u)^2$ and $-4u \notin F(u)^4$. Now if $-4u \in F(u)^4$, then $-4u = k^4$ for some $k \in F(u)$. Then, $k^2 \in F(u)^2$. We also have that $0 \neq 4 = 2^2 \in F(u)^2$. Hence, we should have $-u \in F(u)^2$.

Now we claim

$$-u \in F(u)^2 \iff u \in F(u)^2.$$

We know that the map $\sigma : F(u) \rightarrow F(u)$, where $\sigma(u) = -u$, is an element of $\text{Gal}(F(u)/F)$. Suppose that $u \in F(u)^2$. Then, there exists $z \in F(u)^2$, such that $u = z^2$. Now we obtain

$$\sigma(u) = -u = \sigma(z^2) = \sigma(z)^2.$$

But $\sigma(z)$ is an element of $F(u)$. Thus, we obtain $-u \in F(u)^2$. Reverse implication can be shown in a similar way. Hence, we can say that

$$u \notin F(u)^2 \implies -4u \notin F(u)^4.$$

We have

$$u \notin F(u)^2 \text{ and } -4u \notin F(u)^4 \iff u \notin F(u)^2.$$

But we assumed that $-4a \notin F^4$. Hence by Lemma 3.1.3 (2), we have $u \notin F(u)^2$. Therefore, $X^{2^{n-1}} - u \in F(u)[X]$ is irreducible over $F(u)$, and this implies that $X^{2^n} - a$ is irreducible over F . Hence we have proven (2). \square

Now we can state and prove The Vahlen-Capelli Criterion. But before proving that, let us define the set $-4F^4$. We have $-4F^4 := \{-4b^4 \mid b \in F\}$.

Theorem 3.1.5. (*The Vahlen-Capelli Criterion*) Let F be an arbitrary field, and let $n \in \mathbb{N}^*$, and let $a \in F$. Then the followings are equivalent.

(1) The polynomial $X^n - a$ is irreducible in $F[X]$.

(2) $a \notin F^p$ for all $p \in \mathbb{P}_n$ and $a \notin -4F^4$ whenever $4 \mid n$.

Proof. (1) \implies (2) : For $n = 1$, there is nothing to prove, since $X - a$ is irreducible over F . So we can assume that $n \geq 2$. Now let p be a prime divisor of n . Then $p \in \mathbb{P}_n$. If we have $a \in F^p$, then $a = b^p$ for some $b \in F$. So we have, $X^n - a = (X^m)^p - b^p$, where $n = pm$. But this implies that $X^m - b \in F[X]$ divides $X^n - a$. Hence, $X^n - a$ is reducible over F .

If $4 \mid n$ and $a \in -4F^4$, then $a = -4b^4$, for some $b \in F$; and $n = 4k$, for some $k \in \mathbb{Z}$. Then we have,

$$X^n - a = (X^{2k})^2 + (2b^2)^2 = (X^{2k} + 2b^2)^2 - (2bx^k)^2 = (X^{2k} - 2bx^k + 2b^2)(X^{2k} + 2bx^k + 2b^2)$$

Thus, $X^n - a$ is reducible over F . This proves (1) \implies (2).

(2) \implies (1) : Conversely, assume that (2) holds. Let

$$n = p_1^{k_1} \dots p_r^{k_r}$$

be the decomposition of n as a product of distinct prime numbers p_1, p_2, \dots, p_r with $r, k_1, k_2, \dots, k_r \in \mathbb{N}^*$. By Lemma 3.1.1, in order to show that $X^n - a$ is irreducible over F , it is enough to check that $X^{p_i^{k_i}} - a$ is irreducible over F , for all $i \in \{1, 2, \dots, r\}$. But this follows from Lemma 3.1.4 and the fact that $\text{Char}(F) \neq 2$ and $a \notin -4F^4$ implies that $-4a \notin F^4$.

If this is not the case, then we have $-4a = b^4$, for some $b \in F$. Since $\text{Char}(F) \neq 2$, we have $b = 2c$ for some $c \in F^*$. Then we have $-4a = (2c)^4 = 16c^4$. This implies that $a = -4c^4$. But this leads to a contradiction, since $a \notin -4F^4$. Hence we have shown that $X^n - a$ is irreducible in $F[X]$. This proves (2) \implies (1). \square

Now the following result is an alternative version of the Vahlen-Capelli Criterion.

Proposition 3.1.6. (A Variant of the Vahlen-Capelli Criterion) *Let F be an arbitrary field, let $n \in \mathbb{N}$, $n \geq 2$, and let $a \in F^*$. Then the polynomial $X^n - a$ is reducible in $F[X]$ if and only if one of the following two conditions are satisfied.*

- (1) $a \in F^s$ for some $s \in \mathbb{N}$, $s \geq 2$, $s \mid n$, or
- (2) $4 \mid n$ and $-4a \in F^{*4}$.

Proof. We can easily see that for any $a \in F^*$, we have

$$-4a \in F^{*4} \iff a \in -4F^{*4}.$$

We have shown the implication (\implies) in the proof of The Vahlen-Capelli Criterion. But we can clearly show the reverse implication.

If we take the negation of Theorem 3.1.5, then we have that $X^n - a$ is reducible over F if and only if either $a \in F^p$ for some prime divisor p of n , or $-4a \in F^{*4}$, whenever $4 \mid n$.

If we take a divisor s of n as prime in (1) above, we can see that the negation of The Vahlen-Capelli Criterion and Proposition 3.1.6 are equivalent. Hence this proves Proposition 3.1.6. \square

Remark 3.1.7. The negation of The Vahlen-Capelli Criterion does not say that $X^n - a$ is reducible over F if and only if either $a \in F^p$ for some prime divisor p of n , or $4 \mid n$ and $-4a \in F^4$. If we take F as any non perfect field of characteristic 2, then $F^2 \neq F$, and $F^2 \subseteq F$. Let $F = \mathbb{F}_2(Y) = \{f(Y)/g(Y) \mid f, g \in \mathbb{F}_2[Y]\}$. Clearly, F is non perfect. If $F = F^2$, then $Y \in F^2$. So, we have

$$Y = (f(Y)/g(Y))^2 = (a_0 + a_1Y + \dots + a_nY^n)^2 / (b_0 + b_1Y + \dots + b_mY^m)^2,$$

where $f(Y), g(Y) \in \mathbb{F}_2[Y]$ and $a_n, b_m \neq 0$. Then we have

$$a_0^2 + a_1^2Y^2 + \dots + a_n^2Y^{2n} = b_0^2Y + b_1^2Y^3 + \dots + b_m^2Y^{2m+1},$$

since $\text{Char}(F) = 2$. But this is a contradiction, since the degrees do not match. Hence F is a non perfect field, that is $F \neq F^2$. Now let $a \in F \setminus F^2$, and consider the

polynomial $X^4 - a$. According to Theorem 3.1.5, we have that $X^4 - a$ is irreducible, since $a \notin F^2$ and $a \notin -4F^4 = \{0\}$. But we also have $-4a = 0 \in F^4$. This shows that $X^4 - a$ is reducible over F , according to the negation of the Vahlen-Capelli Criterion above. But this leads to a contradiction. \square

Now we try to put some conditions on the field F or on the binomial $X^n - a$ in order to make the condition

$$a \notin -4F^4 \text{ whenever } 4 \mid n$$

more accurate.

Definition 3.1.8. *The field F is said to satisfy the condition $C_0(n; a)$ (resp. $C_1(n; a)$), where $n \in \mathbb{N}^*$ and $a \in F^*$, if the binomial $X^n - a$ has a root in Ω , say $\sqrt[n]{a}$, such that $\mu_n(F(\sqrt[n]{a})) \subseteq F$ (resp. $\mu_n(F(\sqrt[n]{a})) \subseteq \{-1, +1\}$).* \square

Examples 3.1.9. (1) Any field F satisfying the condition $C_1(n; a)$, clearly satisfies the condition $C_0(n; a)$. The field \mathbb{C} satisfies the condition $C_0(n; a)$, for any $n \in \mathbb{N}$, $n \geq 2$ and any $a \in \mathbb{C}^*$, since \mathbb{C} is algebraically closed. But it does not satisfy the condition $C_1(2; -1)$, since $\mu_2(\mathbb{C}) = \{\pm i\} \not\subseteq \{\pm 1\}$.

(2) If $\zeta_n \in F$, for some $n \in \mathbb{N}^*$, where ζ_n is a primitive n -th root of unity, then clearly all the other distinct roots of $X^n - 1$, which are $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ also belongs to F . Hence, $\mu_n(F(\sqrt[n]{a})) \subseteq F$.

(3) Any subfield F of \mathbb{R} satisfies the condition $C_1(n; a)$, for any odd number $n \in \mathbb{N}^*$ and any $a \in F^*$; as well as for any $n \in \mathbb{N}^*$, and any $a \in \mathbb{R}_+^*$.

(4) The field \mathbb{Q} does not satisfy the condition $C_0(4; -4)$. The roots of the polynomial $X^4 + 4$ are $1 + i, 1 - i, -1 + i, -1 - i$. If $\sqrt[4]{-4}$ denotes any of these roots, then we have $\mathbb{Q}(\sqrt[4]{-4}) = \mathbb{Q}(i)$. So, all 4-th roots of unity, which are $\pm 1, \pm i$, lie in $\mu_4(\mathbb{Q}(\sqrt[4]{-4}))$. But, $\pm i \notin \mathbb{Q}$. Therefore,

$$\mu_4(\mathbb{Q}(\sqrt[4]{-4})) \not\subseteq \mathbb{Q}.$$

Thus, \mathbb{Q} does not satisfy the condition $C_0(4; -4)$. \square

Proposition 3.1.10. *The following assertions hold for a field F satisfying the condition $C_0(n, a)$.*

(1) *The polynomial $X^n - a$ is reducible in $F[X]$ if and only if $a \in F^s$ for some divisor $s > 1$ of n .*

(2) *$\text{Min}(\sqrt[n]{a}, F) = X^m - b$, where $m = \text{ord}(\sqrt[n]{a})$, $m \mid n$ and $b = \sqrt[n]{a}^m$.*

Proof. (1) Let f be the minimal polynomial of $\sqrt[n]{a}$ over F , and let $\deg(f) = m$. Hence, the roots of this polynomial over F are $\sqrt[n]{a}\zeta_n^i \in \Omega$, where $i \in \{0, 1, \dots, m-1\}$. So, the constant term of f is the product of these roots, which is

$$b_0 = \pm \zeta_n^r \sqrt[n]{a}^m,$$

where $r = m(m-1)/2$. Then, we obtain

$$\zeta_n^r = \pm b_0 \sqrt[n]{a}^{-m} \in \mu_n(\Omega) \cap F(\sqrt[n]{a}), \quad (3.1.1)$$

since $(\zeta_n^r)^n = 1$ implies that $\zeta_n^r \in \mu_n(\Omega)$. Because f is a polynomial over F , we have $b_0 \in F$. Also since $F(\sqrt[n]{a})$ is a field, we have $(\sqrt[n]{a})^{-m} \in F(\sqrt[n]{a})$. Therefore, $\zeta_n^r \in F(\sqrt[n]{a})$.

Clearly, $\mu_n(\Omega) \cap F(\sqrt[n]{a}) = \mu_n(F(\sqrt[n]{a}))$. But we know that F satisfies the condition $C_0(n; a)$. Hence $\mu_n(F(\sqrt[n]{a})) \subseteq F$. By Equation (3.1.1), we have $\zeta_n^r \in F$, since $b_0 \in F$. Hence,

$$b = \sqrt[n]{a}^m = \pm b_0 \zeta_n^r \in F.$$

Therefore $X^m - b \in F[X]$. But clearly $\sqrt[n]{a}$ is a root of the polynomial $X^m - b$. Since $\deg(f) = m$, we have $f = \text{Min}(\sqrt[n]{a}, F) = X^m - b$.

If $a \in F^s$ for some divisor $s > 1$ of n , then by Proposition 3.1.6, we have that $X^n - a$ is reducible over F .

Conversely, suppose that $X^n - a$ is reducible over F . Then $1 \leq m = \deg(f) < n$, since f is the minimal polynomial of $\sqrt[n]{a}$ over F . We put $d = \gcd(m, n)$. Then we have $n = ds$ and $m = dt$ for some $s, t \in \mathbb{N}^*$. We know that $\gcd(s, t) = 1$, so there

exists $u, v \in \mathbb{Z}$ such that $ut + vs = 1$. Since $a = \sqrt[t]{a^n} = \sqrt[t]{a^{ds}}$ and $b = \sqrt[m]{a^m} = \sqrt[m]{a^{dt}}$, so we obtain $a^t = b^s$. Thus,

$$a = a^{ut+vs} = (a^t)^u a^{vs} = (b^s)^u a^{vs} = (b^u a^v)^s.$$

But we know that $a, b \in F$. Hence, $a = (b^u a^v)^s \in F^s$. Clearly, $s \mid n$ and $s > 1$. Otherwise if $s = 1$, then $n = \gcd(m, n)$. But this implies that $n \mid m$, and this implies that $n \leq m$. But we have $m < n$. Therefore this proves (1).

(2) We have proved in (1) that $\text{Min}(\sqrt[m]{a}, F) = X^m - b$. Hence it is enough to show that $m = \text{ord}(\sqrt[m]{a})$ and $m \mid n$. Now we show that m is the order of $\sqrt[m]{a}$ in the quotient group $F(\sqrt[m]{a})/F$. Now we put $k = \text{ord}(\sqrt[m]{a})$. Then, $(\sqrt[m]{a})^k = 1$ implies that $c = \sqrt[m]{a}^k \in F$. We know that $(\sqrt[m]{a})^n = a \in F$, so we have $k \mid n$.

Now we claim that $\text{Min}(a, F) = X^k - c$. Then we can say that $k = m$, since

$$\text{Min}(\sqrt[m]{a}, F) = X^m - b = X^m - \sqrt[m]{a}^m.$$

Clearly, $\sqrt[m]{a}$ is a root of $X^k - c$. So it is enough to show that $X^k - c$ is irreducible over F . Suppose that $X^k - c$ is reducible over F . We see that

$$\mu_k(F(\sqrt[m]{a})) \subseteq \mu_n(F(\sqrt[m]{a})) \subseteq F,$$

since $k \mid n$ and F satisfies the condition $C_0(n; a)$. Now we can apply (1) to the polynomial $X^k - c$. Then there exists some $e \in F^*$ such that $c = e^i$, for some divisor $i > 1$ of k . So, we have $k = ij$ where $j \in \mathbb{N}^*$. Then we obtain

$$c = e^i = \sqrt[m]{a}^k = \sqrt[m]{a}^{ij} = (\sqrt[m]{a}^j)^i.$$

Hence, $(\sqrt[m]{a}^j e^{-1})^i = 1$. But this implies that $\sqrt[m]{a}^j e^{-1} \in \mu_i(\Omega)$. Also since

$$\sqrt[m]{a}, e \in F(\sqrt[m]{a}),$$

we obtain $\sqrt[m]{a}^j e^{-1} \in F(\sqrt[m]{a})$. So,

$$\sqrt[m]{a}^j e^{-1} \in \mu_i(\Omega) \cap F(\sqrt[m]{a}) = \mu_i(F(\sqrt[m]{a})) \subseteq \mu_n(F(\sqrt[m]{a})) \subseteq F,$$

since $i | k | n$. Because $e^{-1} \in F^*$, we have $\sqrt[i]{a^j} \in F^*$. But this leads to a contradiction, since $1 \leq j < k$ and $k \in \mathbb{N}^*$ is the least number such that $\sqrt[i]{a^k} \in F$. Therefore,

$$\text{Min}(\sqrt[i]{a}, F) = X^k - c = X^m - b.$$

Thus, $m = k$ and m divides n . This proves (2). \square

Proposition 3.1.11. *Any field F satisfies the condition $C_0(n; a)$ for any $n \in \mathbb{P}$ and any $a \in F^*$.*

Proof. If $n = e(F)$, then for all $x \in \mu_n(\Omega)$, we have $x^n - 1 = 0$. This implies that $(x - 1)^n = 0$, that is $x = 1$. So, $\mu_n(\Omega) = \{1\}$, and we have nothing to prove. Now we may assume that $n \neq e(F)$. We know that

$$\mu_n(F) = \mu_n(\Omega) \cap F^*,$$

and $\mu_n(F)$ is a subgroup of the group $\mu_n(\Omega)$, which has prime order n . Then $\mu_n(F)$ is either $\mu_n(\Omega)$ or $\mu_n(F) = \{1\}$. If $\mu_n(F) = \mu_n(\Omega)$, then we have $\mu_n(\Omega) \subseteq F$.

Now suppose that $\mu_n(F) = \{1\}$. Let $\sqrt[i]{a} \in \Omega$ be a root of the polynomial $X^n - a$. We claim that $\mu_n(F(\sqrt[i]{a})) \neq \mu_n(\Omega)$. Then we can say that $\mu_n(F(\sqrt[i]{a})) = \{1\}$, since $\mu_n(F(\sqrt[i]{a}))$ is a subgroup of $\mu_n(\Omega)$, and $\mu_n(\Omega)$ has prime order.

If $a \in F^n$ then $a = b^n$ for some $b \in F$. Then $F(\sqrt[i]{a}) = F(b) = F$. So,

$$\mu_n(F(\sqrt[i]{a})) = \mu_n(F) = \{1\} \neq \mu_n(\Omega).$$

Now suppose that $a \notin F^n$ and $\mu_n(F(\sqrt[i]{a})) = \mu_n(\Omega)$. Then clearly, $\zeta_n \in \mu_n(\Omega)$ lies in $F(\sqrt[i]{a})$. Hence we obtain $F(\zeta_n) \subseteq F(\sqrt[i]{a})$. Thus,

$$[F(\zeta_n) : F] \mid [F(\sqrt[i]{a}) : F].$$

Since $a \notin F^n$, by Lemma 3.1.2, we have that $X^n - a$ is irreducible over F . Hence, the minimal polynomial of $\sqrt[i]{a}$ over F is $X^n - a$. But this implies that $[F(\sqrt[i]{a}) : F] = n$. Since n is a prime number and

$$[F(\zeta_n) : F] \mid [F(\sqrt[i]{a}) : F]$$

we have $[F(\zeta_n) : F] = 1$. So, $\zeta_n \in F$, and we also have $\zeta_n \in \mu_n(F) = \{1\}$. But this leads to a contradiction, since ζ_n is a primitive n -th root of unity. Therefore we have

$$\mu_n(F(\sqrt[n]{a})) \neq \mu_n(\Omega).$$

This means that $\mu_n(F(\sqrt[n]{a})) = \{1\}$, that is, F satisfies the condition $C_0(n; a)$. \square

3.2 Some Results on Bounded Abelian Groups

In this section, we are going to present some basic properties of Abelian groups of bounded order which will be used in the remaining part of the Thesis. Let G be an arbitrary multiplicative group with identity element e . If $n \in \mathbb{N}^*$, we put $G^n = \{x^n \mid x \in G\}$. For any torsion group G , (a group is said to be a torsion group if every element of it has finite order) we will use the following notation:

$$\mathcal{O}_G = \{\text{ord}(x) \mid x \in G\}.$$

For a nonempty, finite set A of natural numbers, $\text{lcm}(A)$ will denote the least common multiple of all numbers of A , and $\max(A)$ will denote the greatest number of A .

Definition 3.2.1. *A group is said to be a group of bounded order if G is a torsion group and the subset \mathcal{O}_G of \mathbb{N} is a bounded set, or equivalently, a finite set.* \square

It is clear that any finite group is a group of bounded order, and any direct product or direct sum of infinitely many copies of a finite Abelian group of order $n > 1$ is an infinite group of bounded order.

Now we list some results and give a definition which will be needed throughout the remaining part of the Thesis.

Proposition 3.2.2. *If G is an Abelian group of bounded order, and $m = \max(\mathcal{O}_G)$, then $G^m = \{e\}$ and $\text{lcm}(\mathcal{O}_G) \mid m$.* \square

Definition 3.2.3. Let G be a group of bounded order. The least number $n \in \mathbb{N}^*$ with the property that $G^n = \{e\}$ is called the exponent of G and is denoted by $\exp(G)$. The group G is said to be n -bounded if G is a group of bounded order and $\exp(G) = n$. \square

Lemma 3.2.4. Let G be an n -bounded Abelian group. If $G^k = \{e\}$ for some $k \geq 1$, then $n \mid k$. \square

Proposition 3.2.5. Let G be an n -bounded Abelian group. Then, for any $d \in \mathbb{N}$, $d \mid n$ there exists $x_d \in G$ such that $d = \text{ord}(x_d)$. In particular, for every $p \in P_n$ there exists $x_p \in G$ such that $p = \text{ord}(x_p)$. \square

Remark 3.2.6. Proposition 3.2.5 can be reformulated as follows: If G is any n -bounded Abelian group, then $\mathcal{O}_G = \mathbb{D}_n$. \square

Proposition 3.2.7. For any finite Abelian group G , $\exp(G)$ divides $|G|$, and $|G|$ divides a power of $\exp(G)$. In particular, $|G|$ and $\exp(G)$ have the same prime divisors. \square

Lemma 3.2.8. (Cauchy's Lemma) For any finite Abelian group G and any prime divisor p of $|G|$ there exists at least an element $x_p \in G$ with $\text{ord}(x_p) = p$. \square

3.3 Kneser Extensions

In this section we define the G -radical and the G -Kneser extensions. We also give a criterion called the Kneser Criterion which characterizes Kneser extensions.

3.3.1 G -radical and G -Kneser Extensions

For any field extension E/F , we define

$$T(E/F) := \{x \in E^* \mid x^n \in F^* \text{ for some } n \in \mathbb{N}^*\}.$$

Clearly, F^* is a subgroup of $T(E/F)$, so we can consider the quotient group $T(E/F)/F^*$.

For any $x \in E$, we denote by \hat{x} the coset of x modulo F^* in the group E^*/F^* .

By definition of $T(E/F)$ we can see that $T(E/F)/F^*$ is the torsion group of the quotient group E^*/F^* , and it is denoted by $t(E^*/F^*)$. Now we recall that a group G is said to be a torsion group, if all elements of G have finite order.

In the definition below, we give a name to the group $T(E/F)/F^*$, since it plays an important role in this part, similar to that of Galois group in the first part.

Definition 3.3.1. *The Cogalois group of an arbitrary field extension E/F , denoted by $\text{Cog}(E/F)$, is the quotient group $T(E/F)/F^*$.*

A finite extension E/F is said to be a Cogalois extension, if $E = F(T(E/F))$ and $|\text{Cog}(E/F)| = [E : F]$. □

For every $x \in T(E/F)$, there exists $n \in \mathbb{N}^*$ such that $x^n = a \in F^*$. So, as in the Definition 2.7.2, x is denoted as $\sqrt[n]{a}$ and is called the n -th radical of a . Hence, $T(E/F)$ is precisely the set of all “radicals” of elements of F in E .

Definition 3.3.2. *An extension E/F is said to be radical, if there exists $A \subseteq T(E/F)$ such that $E = F(A)$. We say that E/F is a simple radical extension, if there exists an $a \in T(E/F)$ such that $E = F(a)$.* □

Definition 3.3.3. *Let E/F be an extension and let G be a group. Then E/F is said to be a G -radical extension, if $F^* \leq G \leq T(E/F)$ and $E = F(G)$.* □

Remarks 3.3.4. (1) Clearly, any G -radical extension E/F is also G' -radical extension, for any G' with $G \leq G' \leq T(E/F)$.

(2) Let $F \subseteq K \subseteq E$ be a tower of fields. If E/F is a radical extension, then so is E/K , and we have $E = F(A)$, where $A \subseteq T(E/F)$. But $E = F(A) \subseteq K(A) \subseteq E$, so we have $E = K(A)$. Hence, E/K is also radical extension. But later we will see that in general, K/F is not a radical extension.

(3) Any radical extension is algebraic, by definition of a radical extension. So, if E/F is a G -radical extension, then $E = F(G) = F[G]$. □

Lemma 3.3.5. *Let E/F be a G -radical extension, which is not necessarily finite. Then any set of representatives of the factor group G/F^* is a set of generators of the*

F -vector space E . In particular, one has

$$|G/F^*| \geq [E : F].$$

Proof. Because, E/F is G -radical, we have $E = F(G) = F[G]$. Let $T = \{t_i \mid i \in I\}$ be a set of representatives of the factor group G/F^* . Then $G/F^* = \{\widehat{t}_i \mid i \in I\}$. For each $x \in E$, there exists $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ and $g_1, g_2, \dots, g_n \in G$ such that $x = \sum_{k=1}^n \alpha_k g_k$. Clearly, $\widehat{g}_k \in G/F^*$ for all k . Then, we have $g_k = \beta_k t_{i_k}$, where $\beta_k \in F^*$, for all k .

Thus,

$$x = \sum_{k=1}^n \alpha_k g_k = \sum_{k=1}^n (\alpha_k \beta_k) t_{i_k} = \sum_{k=1}^n \delta_k t_{i_k},$$

where $\delta_k = \alpha_k \beta_k \in F$. Hence, T is a set of generators of the F -vector space E . \square

Next we give a corollary that can be shown using Lemma 3.3.5.

Corollary 3.3.6. *Let E/F be a finite G -radical extension. Then there exists a subgroup H of G such that H/F^* is a finite group and E/F is H -radical. \square*

Proposition 3.3.7. *The following statements are equivalent for an arbitrary G -radical extension E/F .*

- (1) *There exists a set of representatives of the factor group G/F^* which is linearly independent over F .*
- (2) *Every set of representatives of G/F^* is linearly independent over F .*
- (3) *Every set of representatives of G/F^* is a vector space basis of E over F .*
- (4) *There exists a set of representatives of G/F^* which is a vector space basis of E over F .*
- (5) *Every subset of G consisted of elements having distinct cosets in the group G/F^* is linearly independent over F .*
- (6) *Every finite subset $\{x_1, x_2, \dots, x_n\} \subseteq G$ such that $\widehat{x}_i \neq \widehat{x}_j$ for each $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, is linearly independent over F .*

(7) For every subgroup H of G such that $F^* \leq H$ and H/F^* is a finite group,

$$|H/F^*| \leq [F(H) : F].$$

Proof. We only prove (7) \implies (2), since other parts can be shown in a similar way.

(3) \implies (4), (4) \implies (1) and (5) \iff (6) are obvious and (2) \implies (3) follows from Lemma 3.3.5. Assume that (7) holds. Let $T = \{t_i \mid i \in I\}$ be a set of representatives of the factor group G/F^* and let $\{t_1, t_2, \dots, t_n\}$ be a finite subset of T . Now consider the subgroup $\langle \widehat{t}_1, \widehat{t}_2, \dots, \widehat{t}_n \rangle$ of the group G/F^* , generated by $\{\widehat{t}_1, \widehat{t}_2, \dots, \widehat{t}_n\}$. Since we have $G \leq T(E/F)$, for all $i \in \{1, 2, \dots, n\}$, \widehat{t}_i has finite order. So the subgroup generated by $\{\widehat{t}_1, \widehat{t}_2, \dots, \widehat{t}_n\}$ has also finite order since

$$|\langle \widehat{t}_1, \widehat{t}_2, \dots, \widehat{t}_n \rangle| \leq \text{ord}(\widehat{t}_1) \text{ord}(\widehat{t}_2) \dots \text{ord}(\widehat{t}_n).$$

Now since $\langle \widehat{t}_1, \widehat{t}_2, \dots, \widehat{t}_n \rangle$ is a subgroup of G/F^* , we have $\langle \widehat{t}_1, \widehat{t}_2, \dots, \widehat{t}_n \rangle = H/F^*$, for some $H \leq G$ with $F^* \leq H$. By assumption we have $|H/F^*| \leq [F(H) : F]$. Clearly $F(H)/F$ is an H -radical extension, since

$$F^* \leq H \leq G \leq T(E/F).$$

So we can apply Lemma 3.3.5 to the extension $F(H)/F$. Then $|H/F^*| \geq [F(H) : F]$.

Thus we have

$$|H/F^*| = [F(H) : F].$$

This implies that any set of representatives of the group H/F^* is a vector space basis of $F(H)$ over F , that is, any set of representatives of the group H/F^* is linearly independent. So, $\{t_1, t_2, \dots, t_n\}$ is linearly independent over F . Since any finite subset of T is linearly independent over F , we have that T is linearly independent over F . \square

Now we define G -Kneser extensions which we have mentioned at the beginning of this section.

Definition 3.3.8. A finite extension E/F is said to be G -Kneser, if it is a G -radical extension such that $|G/F^*| \geq [E : F]$. The extension E/F is called Kneser, if it is G -Kneser for some group G . \square

Corollary 3.3.9. *The following assertions are equivalent for a finite G -radical extension E/F .*

- (1) E/F is G -Kneser.
- (2) $|G/F^*| = [E : F]$.
- (3) Every set of representatives of G/F^* is a vector space basis of E over F .
- (4) There exists a set of representatives of G/F^* which is linearly independent over F .
- (5) Every finite subset $\{x_1, x_2, \dots, x_n\} \subseteq G$ such that $\hat{x}_i \neq \hat{x}_j$ for each $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, is linearly independent over F .
- (6) The extension $F(H)/F$ is H -Kneser for every H , $F^* \leq H \leq G$.

Proof. By Lemma 3.3.5 we can see that (1) \iff (2). (2) \implies (3), (3) \iff (4) and (4) \implies (5) follows from Proposition 3.3.7. (5) \implies (6) follows both from Lemma 3.3.5 and Proposition 3.3.7. If we take $H = G$, (6) \implies (1) can be shown. \square

Proposition 3.3.10. *Let E/F be a finite G -Kneser extension. Then, the extension $F(H)/F$ is H -Kneser and $F(H) \cap G = H$ for every H with $F^* \leq H \leq G$.*

Proof. By Corollary 3.3.9, we have that $F(H)/F$ is H -Kneser. Clearly, we have $H \subseteq F(H) \cap G$. Now we have to show the other inclusion. Let $x \in F(H) \cap G$, then we have

$$x = \alpha_1 h_1 + \alpha_2 h_2 + \dots + \alpha_k h_k, \quad (3.3.1)$$

where $\alpha_i \in F$ and $h_i \in H$ for all i . We can take $\hat{h}_i \neq \hat{h}_j$, for all $i, j \in \{1, 2, \dots, k\}$ in $H/F^* \subseteq G/F^*$. Equation (3.3.1) implies that x, h_1, h_2, \dots, h_k are linearly dependent over F .

So, from Corollary 3.3.9, we can say that there exists at least two equal cosets. But we have assumed that $h_i \neq h_j$, for all i, j . So, we should have $\hat{x} = \hat{h}_j$ for some

j. But, this implies that $x = \alpha h_j$, $\alpha \in F^*$. Thus $x \in H$, since $F^* \leq H$. Therefore we have $F(H) \cap G \subseteq H$. \square

Remark 3.3.11. (1) Any Cogalois extension E/F is clearly a Kneser extension. If we put $G = T(E/F)$, we can see that any Cogalois extension E/F is a $T(E/F)$ -Kneser extension. But the converse of this statement does not hold.

Consider the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. This extension is $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -Kneser,¹ but it is not a Cogalois extension. Since $\zeta_3, \zeta_3^2 \notin \mathbb{Q}^*$, and $\zeta_3^3 = 1 \in \mathbb{Q}^*$; we have $\widehat{\zeta_3^3} = \widehat{1}$, and $\widehat{1}, \widehat{\zeta_3}, \widehat{\zeta_3^2} \in \mathbb{Q}^*\langle\zeta_3\rangle/\mathbb{Q}^*$. Hence

$$\mathbb{Q}^*\langle\zeta_3\rangle/\mathbb{Q}^* = \{\widehat{1}, \widehat{\zeta_3}, \widehat{\zeta_3^2}\}.$$

We know that

$$\text{Cog}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) = T(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})/\mathbb{Q}^* = t(\mathbb{Q}(\sqrt{-3})^*/\mathbb{Q}^*).$$

We have that $\zeta_3 \in \mathbb{Q}^*(\sqrt{-3})$. Since ζ_3 is a primitive third root of unity, it is a root of the polynomial $X^2 + X + 1 \in \mathbb{Q}[X]$. But we also have $\zeta_3^3 = 1$. Hence the order of ζ_3 is finite in $\mathbb{Q}^*(\sqrt{-3})$. Thus, $\widehat{\zeta_3} \in t(\mathbb{Q}^*(\sqrt{-3})/\mathbb{Q}^*)$. Hence $\langle\widehat{\zeta_3}\rangle \leq t(\mathbb{Q}^*(\sqrt{-3})/\mathbb{Q}^*)$. Therefore, $\langle\zeta_3\rangle = \mathbb{Q}^*\langle\zeta_3\rangle/\mathbb{Q}^* \leq \text{Cog}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$. Thus,

$$|\text{Cog}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})| \geq 3 > 2 = |\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}|,$$

since the order of the group $\mathbb{Q}^*\langle\zeta_3\rangle/\mathbb{Q}^*$ is 3. But this shows that the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is not a Cogalois extension.

On the other hand, this extension is $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -Kneser. In order to show this, we have to have $|\mathbb{Q}^*\langle\sqrt{-3}\rangle/\mathbb{Q}^*| = |\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}|$. But we know that $|\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}| = 2$, so it is enough to show that $|\mathbb{Q}^*\langle\sqrt{-3}\rangle/\mathbb{Q}^*| = 2$. We have $(\sqrt{-3})^2 = -3 \in \mathbb{Q}^*$, so $\widehat{(\sqrt{-3})^2} = \widehat{1}$.

Thus we obtain

$$\mathbb{Q}^*\langle\sqrt{-3}\rangle/\mathbb{Q}^* = \{\widehat{1}, \widehat{\sqrt{-3}}\},$$

¹ $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ is the subgroup of the multiplicative group \mathbb{C}^* of \mathbb{C} , which is generated by \mathbb{Q}^* and $\sqrt{-3}$.

and this implies that $|\mathbb{Q}^*\langle\sqrt{-3}\rangle/\mathbb{Q}^*| = 2$.

Hence, $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -Kneser extension. \square

3.3.2 The Kneser Criterion

The Kneser Criterion is one of the most important theorems in this section, since it characterizes the separable Kneser extensions.

Theorem 3.3.12: (*The Kneser Criterion*) *The following assertions are equivalent for a separable G -radical extension E/F with finite G/F^* .*

- (1) E/F is a G -Kneser extension.
- (2) For every odd prime p , $\zeta_p \in G \implies \zeta_p \in F$, and $1 + \zeta_4$ or $1 - \zeta_4 \in G \implies \zeta_4 \in F$.
- (3) $\mu_p(G) = \mu_p(F)$ for every odd prime p , and $1 + \zeta_4$ or $1 - \zeta_4 \in G \implies \zeta_4 \in F$.

Proof. Since E/F is a G -radical extension, we have $E = F(G)$. Also G/F^* is given to be a finite group, so we have that E/F is a finite extension.

(2) \implies (3) : Assume that (2) holds. Then we have, for every odd prime p ,

$$\zeta_p \in G \implies \zeta_p \in F.$$

Now we have to show that $\mu_p(G) = \mu_p(F)$. Let $x \in \mu_p(G)$, we have $x^p = 1$. So, the order of $x \in G$ is either 1 or p , since p is prime.

If the order of x is 1, then $x = 1$, which means that $x \in F$. Therefore $x \in \mu_p(F)$. If $\text{ord}(x) = p$, then $\langle x \rangle = \langle \zeta_p \rangle$, since ζ_p is a primitive p -th root of unity. Because $x \in G$, we have $\langle x \rangle \leq G$. Also we have $\zeta_p \in \langle x \rangle \leq G$. Now by our assumption, we obtain $\zeta_p \in F$. But this implies that $x \in \langle \zeta_p \rangle \leq F$. Hence $x \in \mu_p(F)$. The other inclusion is clear, since $F^* \leq G$. Thus, $\mu_p(F) = \mu_p(G)$.

(3) \implies (2) : Now assume that (3) holds. Then clearly we have that for any odd prime p , $\zeta_p \in G \implies \zeta_p \in F$. Since the other parts are the same, there is nothing to prove. \square

(1) \implies (2) : If $\text{Char}(F) = 2$, then $\zeta_4 = 1$. Hence, $1 + \zeta_4 \in G \iff 1 - \zeta_4 \in G$.

If $\text{Char}(F) \neq 2$, and $1 + \zeta_4 \in G$, then $(1 + \zeta_4)^2 = 2\zeta_4 \in G$. But $2 \in F^* \leq G$, so if we multiply the above equation by the inverse of 2, then we obtain $\zeta_4 \in G$. So,

$$\zeta_4(1 + \zeta_4) = \zeta_4 + \zeta_4^2 = -1 + \zeta_4 \in G,$$

since $\zeta_4 \neq \pm 1$ is a root of the polynomial $X^4 - 1 = (X^2 + 1)(X^2 - 1) \in F[X]$. We also have that $-1 \in G$, since $-1 \in F^* \leq G$. So we obtain $(-1)(-1 + \zeta_4) = 1 - \zeta_4 \in G$. The other implication can similarly be shown.

Now suppose that the extension E/F is G-Kneser and p is an odd prime such that $\zeta_p \in G$. Our aim is to show that $\zeta_p \in F$. We have $\widehat{\zeta}_p^p = 1$, so the order of $\widehat{\zeta}_p \in G/F^*$ is 1 or p .

If $\text{ord}(\widehat{\zeta}_p) = p$, then the cosets $\widehat{1}, \widehat{\zeta}_p, \dots, \widehat{\zeta}_p^{p-1}$ are distinct in the group G/F^* . So by Corollary 3.3.9, we can say that $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\} \subseteq G$ is linearly independent over F . But ζ_p is a primitive p -th root of unity, so $\zeta_p \neq 1$. We also have

$$\zeta_p^p - 1 = (\zeta_p - 1)(\zeta_p^{p-1} + \zeta_p^{p-2} + \dots + \zeta_p + 1) = 0.$$

This shows that

$$\zeta_p^{p-1} + \zeta_p^{p-2} + \dots + \zeta_p + 1 = 0.$$

But we know that the subset $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$ of G is linearly independent. So, this leads to a contradiction. Hence, $\text{ord}(\widehat{\zeta}_p) = 1$ in G/F^* . Hence $\widehat{\zeta}_p = \widehat{1}$, so $\zeta_p \in F^*$. Therefore we have proven the first part of (2).

Now we show the second part of (2). If we have $1 + \zeta_4 \in G$, then we have to consider two cases:

i) If $\text{Char}(F) = 2$, then $\zeta_4^4 = 1$ implies that $\zeta_4 = 1$, that is $\zeta_4 \in F$.

ii) Suppose that $\text{Char}(F) \neq 2$. We have shown above that $(1 + \zeta_4)^2 = 2\zeta_4$ and $\zeta_4^2 = -1$. So, we can deduce that

$$(1 + \zeta_4)^4 = ((1 + \zeta_4)^2)^2 = 4\zeta_4^2 = -4 \in F^*.$$

This implies that $\text{ord}(\widehat{1 + \zeta_4}) \in \{1, 2, 4\}$ in G/F^* .

If $\text{ord}(\widehat{1 + \zeta_4}) = 1$, then $1 + \zeta_4 \in F^*$. But this shows that $\zeta_4 \in F$.

If $\text{ord}(\widehat{1 + \zeta_4}) = 2$, then $(1 + \zeta_4)^2 \in F^*$. We have $(1 + \zeta_4)^2 = 2\zeta_4$, so, $2\zeta_4 \in F^*$. But since F is a field and $\text{Char}(F) \neq 2$, we have $2^{-1} \in F$. Hence, $\zeta_4 \in F$.

If $\text{ord}(\widehat{1 + \zeta_4}) = 4$, then the cosets

$$\widehat{1}, \widehat{1 + \zeta_4}, \widehat{(1 + \zeta_4)^2}, \widehat{(1 + \zeta_4)^3}$$

are distinct in the group G/F^* . So by Corollary 3.3.9, the set

$\{\widehat{1}, \widehat{1 + \zeta_4}, \widehat{(1 + \zeta_4)^2}, \widehat{(1 + \zeta_4)^3}\}$ is linearly independent over F . But this leads to a contradiction, since we have

$$2.1 + (-2)(1 + \zeta_4) + (1 + \zeta_4)^2 + 0.(1 + \zeta_4)^3 = 0.$$

Thus, we conclude that the order of $\widehat{1 + \zeta_4}$ can not be equal to 4. Hence, $\text{ord}(\widehat{1 + \zeta_4})$ should be 1 or 2. Therefore, we obtain $\zeta_4 \in F$, as we have shown above. At the beginning of the proof of (1) \implies (2), we have shown that $1 + \zeta_4 \in G \iff 1 - \zeta_4 \in G$ held in the above two cases. So, we have proven (1) \implies (2).

(2) \implies (1) : Now suppose that (2) holds. By Lemma 3.3.5, we have

$$|G/F^*| \geq [E : F],$$

so it is enough to show that $|G/F^*| \leq [E : F]$. We can assume that $|G/F^*| \geq 2$.

Firstly, we consider the case, where G/F^* is a p -group, then we generalize this fact. Since G/F^* is a finite group, we may assume that $|G/F^*| = p^t$, where $p \in \mathbb{P}$ and $t \in \mathbb{N}^*$. Then by the First Sylow Theorem², we know that there is a chain of subgroups H_i/F^* of order p^i , where $1 \leq i \leq t$. Then we have

$$F^* = H_0 \leq H_1 \leq \dots \leq H_t = G,$$

where $|H_k/H_{k-1}| = p$ for all $k = 1, 2, \dots, t$. The equality $|H_k/H_{k-1}| = p$ comes from the fact that $H_k/F^*/H_{k-1}/F^*$ is isomorphic to H_k/H_{k-1} . Now by induction on k , $0 \leq k \leq t$, we prove that the following two statements hold.

²First Sylow Theorem: Let $|G| = mp^n$, where n is positive and p does not divide m . For each $i \in \{1, 2, \dots, n\}$ there is a subgroup of order p^i , and if $i < n$, each subgroup of order p^i is normal in a subgroup of order p^{i+1} .

(A_k) $[F(H_k) : F(H_{k-1})] = p$.

(B_k) If $p > 2$, and $c \in F(H_k)$ with $c^p \in H_k$, then $c \in H_k$.

If $p = 2$, and $c \in F(H_k)$ with $c^2 \in H_k$, and either $c \in G$ or $\zeta_4 \notin F(H_k)$, then $c \in H_k$.

For $k = 0$, we can see that (A_0) is not defined and (B_0) holds, since $H_0 = F^*$. So we may assume that $k \geq 1$. Now we suppose that (B_{k-1}) holds. We show that (B_{k-1}) implies that (A_k). Since $|H_k/H_{k-1}| = p$, it follows that H_k/H_{k-1} is a cyclic group. Let $\hat{a} = aH_{k-1}$ be a generator of this cyclic group. Then $a \notin H_{k-1}$, and $\hat{a}^p = \hat{1}$, which means that $(aH_{k-1})^p = H_{k-1}$. So, $a^p \in H_{k-1}$. Now we have

$$a \in H_k \setminus H_{k-1}, H_k = H_{k-1}\langle a \rangle, \text{ and } a^p \in H_{k-1}.$$

Clearly, a is a root of the polynomial $g = X^p - a^p \in F(H_{k-1})[X]$. We show that this polynomial is the minimal polynomial of a over $F(H_{k-1})$. Then we obtain

$$[F(H_k) : F(H_{k-1})] = p,$$

as desired. So it is enough to show that $g = X^p - a^p$ is irreducible over $F(H_{k-1})$.

Now we suppose that g is reducible over $F(H_{k-1})$, and end up with a contradiction. By Lemma 3.1.2, we can say that $a^p \in F(H_{k-1})^p$. Then there exists $b \in F(H_{k-1})$ such that $a^p = b^p$. But this implies that $b \in F(H_{k-1})$ is a root of the polynomial g . We also have $b^p = a^p \in H_{k-1}$.

If $p > 2$, then we have $b \in H_{k-1}$ by (B_{k-1}). We know that b is a root of the polynomial g . So, b is of the form $a\zeta_p$, with $a \in H_k$. Since $b \in H_{k-1} \leq H_k$, we have

$$\zeta_p = a^{-1}b \in H_k \leq G.$$

But we have (2), so $\zeta_p \in F$. But this implies that $a = b\zeta_p^{-1} \in H_{k-1}$, since $F^* \leq H_{k-1}$. But this contradicts the fact that $a \in H_k \setminus H_{k-1}$.

If $p = 2$, then $a^2 = b^2$ implies that $a = \pm b$. So, $b \in H_k$, since $a \in H_k \leq G$. Again using (B_{k-1}), and knowing that $b \in G$ and $a^2 = b^2 \in H_{k-1}$, we can conclude that $b \in H_{k-1}$. This implies that $a \in H_{k-1}$, but this contradicts the choice of a . Hence, for all prime p , $g = X^p - a^p$ is irreducible over $F(H_{k-1})$. Therefore, (A_k) holds.

Now we have both (A_k) and (B_{k-1}) . Our aim is to show that (B_k) holds. We consider two cases, where p is an even or an odd prime.

Case I:

Suppose that $p > 2$. Let $c \in F(H_k)$, with $c^p \in H_k$. We have to show that $c \in H_k$. Since $c^p \in H_k$, we have $\widehat{c^p} \in H_k/H_{k-1}$. We have that \widehat{a} is a generator of the cyclic group H_k/H_{k-1} of order p . Then, we have $\widehat{c^p} = \widehat{a}^q$, where $0 \leq q \leq p-1$. Now we can write

$$c^p = a^q d,$$

where $d \in H_{k-1}$.

First suppose that $q > 0$. We know that

$$F(H_k) = F(H_{k-1}\langle a \rangle) = (F(H_{k-1}))\langle a \rangle.$$

A $F(H_k)$ -homomorphism should send the roots of g to themselves by Lemma 2.6.2, so,

$$N(a) = a \cdot (a\zeta_p) \cdot (a\zeta_p^2) \cdots (a\zeta_p^{p-1}) = a^p \cdot \zeta_p^{(p-1)p/2} = a^p,$$

since $p > 2$ and ζ_p is a primitive p -th root of unity. Now we can write

$$a^q = c^p d^{-1}.$$

If we take the norms of both sides of this equation, we obtain

$$N(a^q) = N(c^p)N(d^{-1}),$$

since the norm function is multiplicative (We have defined the “norm” of an element in a field extension in the Definition 2.7.1). Then we have

$$(a^p)^q = (N(c)d^{-1})^p. \tag{3.3.2}$$

But $1 \leq q < p$, so p and q are relatively prime integers. Then, there exists some $u, v \in \mathbb{Z}$ such that $up + vq = 1$. Hence, we have

$$a^p = (a^p)^1 = ((a^p)^u)^p ((a^p)^q)^v = ((a^p)^u)^p (N(c)d^{-1})^v.$$

But we know that $a^p, N(c)d^{-1} \in F(H_{k-1})$, so a^p can be written as a p -th power of an element from the field $F(H_{k-1})$. But this leads to a contradiction, since

$$g = X^p - a^p \in F(H_{k-1})[X]$$

is irreducible over $F(H_{k-1})$. But by the above result and Lemma 3.1.2, we have that $g = X^p - a^p$ is reducible over $F(H_{k-1})$.

So we cannot have $q > 0$. Therefore, $q = 0$. So, $c^p = a^q d = d \in H_{k-1}$. If we put $K = F(H_{k-1})$, then $F(H_k) = K(a)$.

Now let L be the normal closure of the extension $K(a)/K$ in Ω . Since E/F is a separable extension, we can say that L/K is also a separable extension. Being the normal closure of a finite extension, L/K is also a finite extension. Also by the definition of normal closure, L/K is normal. Hence, L/K is a Galois extension according to Proposition 2.6.7.

So, $\text{Fix}(\text{Gal}(L/K)) = K$, and for $a \in L \setminus K$, there exists $\varphi \in \text{Gal}(L/K)$ such that $\varphi(a) \neq a$.

Since $a^p \in H_{k-1} \subseteq K$, we have $\varphi(a^p) = a^p = \varphi(a)^p$. So, $(a^{-1}\varphi(a))^p = 1$. Then we can write $a^{-1}\varphi(a) = \zeta_p$. So, we have $\varphi(a) = a\zeta_p$, since $\varphi(a) \neq a$ implies that $a^{-1}\varphi(a) \neq 1$. Then we have that $a^{-1}\varphi(a)$ is a primitive p -th root of unity. Also since $c^p \in H_{k-1} \subseteq K$, we have $\varphi(c^p) = c^p = \varphi(c)^p$. Similarly we have $\varphi(c) = c\zeta_p^m$, where $0 \leq m \leq p-1$. Then we obtain

$$\varphi(a^{-m}c) = \varphi(a)^{-m}\varphi(c) = a^{-m}\zeta_p^{-m}c\zeta_p^m = a^{-m}c.$$

Our aim is to show that $a^{-m}c \in F(H_{k-1}) = K$. So, we should show that $a^{-m}c$ is fixed under every automorphism in the group $\text{Gal}(L/K)$. Now we put $w = a^{-m}c$. Clearly $w \in K(a)$. We know that $[K(a) : K] = p$, so we have

$$w = \sum_{0 \leq i \leq p-1} \lambda_i a^i,$$

where $\lambda_i \in K$. Since $\varphi(a) = a\zeta_p$, we have

$$\varphi(w) = \sum_{0 \leq i \leq p-1} \varphi(\lambda_i)\varphi(a)^i = \sum_{0 \leq i \leq p-1} \lambda_i a^i \zeta_p^i = \sum_{0 \leq i \leq p-1} (\lambda_i \zeta_p^i) a^i = \sum_{0 \leq i \leq p-1} \lambda_i a^i = w. \quad (3.3.3)$$

Since ζ_p is a primitive p -th root of unity, ζ_p is a root of the polynomial

$$X^{p-1} + X^{p-2} + X^{p-3} + \dots + X + 1 \in K[X].$$

Then we have $[K(\zeta_p) : K] \leq p-1$. We also have $[K(a) : K] = p$. But p and the degree of the extension $K(\zeta_p)/K$ are relatively prime, so by Proposition 2.3.6, we have

$$K(a, \zeta_p) : K = [K(\zeta_p) : K] \cdot [K(a) : K].$$

So, we have

$$[K(\zeta_p)(a) : K] = [K(a) : K] = p.$$

In particular, this shows that the set $\{1, a, a^2, \dots, a^{p-1}\}$ which is linearly independent over K , is linearly independent over $K(\zeta_p)$. So, if we put the terms in Equation (3.3.3) together, we have $\lambda_i = \lambda_i \zeta_p^i$, for all $i \in \{0, 1, \dots, p-1\}$. If for all $1 \leq i \leq p-1$, $\lambda_i = 0$ then clearly, $w = \lambda_0 \in K$. Now suppose that $w \notin K$. So, there exists some $1 \leq j \leq p-1$ such that $\lambda_j \neq 0$. Then we have $\lambda_j(1 - \zeta_p^j) = 1$. Now we can divide both sides of the above equation by λ_j , since $\lambda_j \neq 0$. Hence, we obtain $1 = \zeta_p^j$, that is $\zeta_p = 1$. But this is a contradiction, since $\zeta_p \neq 1$.

Therefore, $w = a^{-m}c \in K = F(H_{k-1})$. We have

$$w^p = (a^{-m}c)^p = (a^p)^{-m}c^p \in H_{k-1},$$

since $a^p, c^p \in H_{k-1}$. So by (B_{k-1}) , we can say that $w = a^{-m}c \in H_{k-1}$. Therefore, $c \in H_k$, since $a^m \in H_k$ and $H_{k-1} \leq H_k$. So assuming (B_{k-1}) , we have shown (B_k) .

Case II: Suppose that $p = 2$. Let $c \in F(H_k)$ be such that $c^2 \in H_k$, and either we have $c \in G$ or $\zeta_4 \notin F(H_k)$. We show that $c \in H_k$. Similar to Case I, we have $c^2 = a^q d$, where $d \in H_{k-1}$ and $0 \leq q \leq 1$.

If $q = 1$, then $c^2 = ad$. We take the norm of both sides of the equation, and we obtain

$$N(c)^2 = N(a)N(d).$$

But since $p = 2$ and $N(a) = a^p \zeta_p^{(p-1)p/2}$, we have $N(a) = a^2 \zeta_2 = -a^2$. Clearly, we also have $N(d) = d^2$, since $d \in H_{k-1}$. So,

$$-a^2 = N(c)^2 d^{-2}.$$

Hence we have $-a^2 = (N(c)d^{-1})^2$, where $N(c)d^{-1} \in F(H_{k-1})$. Now put $t = N(c)d^{-1}$. Then we have

$$-a^2 = t^2.$$

We can also write $-1 = (a^{-1}t)^2$, so we have $a^{-1}t = \pm\zeta_4$. Then we can write $a = \pm\zeta_4 t$. But this implies that $\zeta_4 \notin F(H_{k-1})$, since $a \in F(H_{k-1})$. We also have

$$F(H_k) = F(H_{k-1})(a) = F(H_{k-1})(\pm\zeta_4 t) = F(H_{k-1})(\zeta_4),$$

since $t \in F(H_{k-1})$. We know that

$$[F(H_k) : F(H_{k-1})] = [F(H_{k-1}(\zeta_4) : F(H_{k-1}))] = 2,$$

and $c \in F(H_k)$. So, $c = x + y\zeta_4$, where $x, y \in F(H_{k-1})$. Hence we obtain,

$$c^2 = (x + y\zeta_4)^2 = x^2 + 2xy\zeta_4 - y^2 = (x^2 - y^2) + 2xy\zeta_4 = \pm\zeta_4 td,$$

since $\zeta_4^2 = -1$. So, we have $x^2 - y^2 = 0$, which means $x = \pm y$. Thus, we obtain

$$c = x + \zeta_4 y = (1 \pm \zeta_4)x.$$

Clearly, we should have $\text{Char}(F) \neq 2$, otherwise $\zeta_4 = 1$, and this would imply that $a = z \in F(H_{k-1})$. But this contradicts the choice of a .

By our assumption $c^2 \in H_k$. We also have $|H_k : H_{k-1}| = 2$. So, $\widehat{c^2} \in H_k/H_{k-1}$. Then we obtain $(\widehat{c^2})^2 = \widehat{1}$ and this implies that $\widehat{c^4} = \widehat{1}$. So, we have $c^4 \in H_{k-1}$. Now we have $c^4 = (1 \pm \zeta_4)x^4$. But

$$(1 \pm \zeta_4)^4 = ((1 \pm \zeta_4)^2)^2 = (\pm 2\zeta_4)^2 = -4.$$

Then $c^4 = -4x^4$. So, we have

$$x^4 = 4^{-1}(-c^4) \in H_{k-1}.$$

Since $\zeta_4 \notin F(H_{k-1})$, using (B_{k-1}) , we can say that $x^2 \in H_{k-1}$. After applying (B_{k-1}) once more, we obtain $x \in H_{k-1}$. Then $1 \pm \zeta_4 = cx^{-1} \in G$. So, using our assumption in (2), we deduce that $\zeta_4 \in F \subseteq F(H_{k-1})$. But this is a contradiction, since $\zeta_4 \notin F(H_{k-1})$. So we should have $q = 0$ and we obtain $c^2 = d \in H_{k-1}$.

Now we continue as in the Case I. Consider the automorphism

$$\varphi \in \text{Gal}(F(H_k)/F(H_{k-1}))$$

with $\varphi(a) = -a$. We have $\varphi(c^2) = \varphi(c)^2 = c^2$, since $c^2 \in H_{k-1}$. So, $c = \pm\varphi(c)$. If $c = \varphi(c)$, then we take j to be an even integer and if $c = -\varphi(c)$, then we take j to be an odd integer, so we deduce that $\varphi(a^j c) = a^j c$. Similar to the Case I, we can show that $a^j c \in F(H_{k-1})$. Since we have $a^{2j} c^2 \in H_{k-1}$, according to the statement (B_{k-1}) , we have $a^j c \in H_{k-1}$. Hence, $c \in H_k$, since $a^j \in H_k$ and $H_{k-1} \leq H_k$. Therefore, we have proven (B_k) assuming (B_{k-1}) . So, (B_k) is proven inductively. Hence we can say that (A_k) , holds since we have proven that by assuming (B_{k-1}) . Now since $E = F(G) = F(H_k)$, using (A_k) , we deduce that

$$[E : F] = [F(H_k) : F(H_{k-1})] \cdot [F(H_{k-1}) : F(H_{k-2})] \cdots [F(H_1) : F] = p^t = |G/F^*|.$$

Hence, E/F is a G -Kneser extension.

Now suppose that

$$|G/F^*| = p_1^{t_1} \cdots p_r^{t_r},$$

where p_i are mutually distinct prime numbers and $t_i \in \mathbb{N}^*$, $1 \leq i \leq r$. Now let H_i/F^* be a p_i -Sylow subgroup of G/F^* , for all i . Then

$$|H_i/F^*| = p_i^{t_i},$$

for all $1 \leq i \leq r$.

We have shown above that

$$|H_i/F^*| = [F(H_i) : F] = p_i^{t_i}.$$

But we know that $[F(H_i) : F]$ divides the degree of the extension E/F . Then $p_i^{t_i}$ divides $[E : F]$ for all $1 \leq i \leq r$. So, we have that $\prod_{i=1}^r p_i^{t_i}$ divides $[E : F]$. Hence, $|G/F^*|$ divides $[E : F]$. Therefore,

$$|G/F^*| \leq [E : F].$$

So, we have shown that E/F is a G -Kneser extension. Therefore we have proven the Kneser Criterion.

3.4 Cogalois Extensions

In this section we study Cogalois extensions. We have defined Cogalois extensions as finite $T(E/F)$ -Kneser extensions at the beginning of the previous section. In this section we provide the Criterion of Greither and Harrison which characterizes the Cogalois extensions. We also give another criterion, called Gay-Vélez Criterion, which is similar to the Greither-Harrison Criterion. At the end of this section we provide some examples concerning Cogalois extensions.

3.4.1 The Greither-Harrison Criterion

Before proving the criterion, we need to define some concepts. Firstly, we recall the concept of *purity* in Group Theory. A subgroup H of an Abelian multiplicative group G is called *pure*, if $G^n \cap H = H^n$, for every $n \in \mathbb{N}^*$. Then we give the definition of a pure extension.

Definition 3.4.1. *An extension E/F is said to be pure, if $\mu_p(E) \subseteq F$ for every $p \in \mathcal{P}$.* □

Lemma 3.4.2. *The following assertions are equivalent for an extension E/F .*

- (1) E/F is pure.
- (2) $\mu_p(E) = \mu_p(F)$ for every $p \in \mathcal{P}$.
- (3) $\zeta_p \in E \implies \zeta_p \in F$ for every $p \in \mathcal{P}$.
- (4) $\zeta_{2p} \notin E \setminus F$ for every $p \in \mathbb{P}$.

Proof. Since $\mu_p(F) \subseteq F$, we can see that (1) \iff (2) and (2) \implies (3) hold. We first show that (3) \implies (1).

(3) \implies (1) : Now assume that (3) holds, and let $\zeta \in \mu_p(E)$. Then $\zeta^p = 1$, so the order of the element $\zeta \in E^*$ is a divisor of p . If p is an odd prime, then $\text{ord}(\zeta)$ is

either 1 or p . If $\text{ord}(\zeta) = 1$, then $\zeta = 1 \in F$, as desired. If $\text{ord}(\zeta) = p$, then ζ is a generator of $\mu_p(E)$. Then $\langle \zeta \rangle = \langle \zeta_p \rangle$ in Ω^* . Thus, $\zeta_p \in \langle \zeta \rangle \leq E^*$. So, according to our assumption, we obtain $\zeta_p \in F$. Then, $\zeta \in \langle \zeta_p \rangle \leq F^*$. So, we obtain $\zeta \in F$, as desired.

Now assume that $p = 4$, then $\zeta^4 = 1$. So, $\text{ord}(\zeta) \in \{1, 2, 4\}$. If $\text{ord}(\zeta) = 1$, then $\zeta = 1 \in F$. If $\text{ord}(\zeta) = 2$, then $\zeta = -1 \in F$. If $\text{ord}(\zeta) = 4$, then similar to the case where p is an odd prime, we have $\zeta \in F$. Therefore, E/F is a pure extension.

(3) \iff (4) : If $\text{Char}(F) = 2$, then we have $\zeta_4 = 1$, and ζ_{2p} is a primitive p -th root of unity for every odd prime p . It is clear that $\zeta_4 = 1$. We know that $\zeta_{2p}^{2p} = 1$, so we can write it as $((\zeta_{2p})^p)^2 - 1 = 0$. Since $\text{Char}(F) = 2$, we have

$$((\zeta_{2p})^p - 1)^2 = 0.$$

Then we have $(\zeta_{2p})^p = 1$. So the order of $\zeta_{2p} \in \Omega^*$ is 1 or p . But we know that $\zeta_{2p} \neq 1$, so $\text{ord}(\zeta_{2p}) = p$, and this implies that ζ_{2p} is a primitive p -th root of unity for every odd prime p .

Now consider the case where $\text{Char}(F) \neq 2$. We want to show that $-\zeta_{2p}$ is a primitive p -th root of unity for every odd prime p . We have

$$((\zeta_{2p})^p)^2 = 1,$$

since the order of ζ_p is $2p$. Then $(\zeta_{2p})^p = -1$. We have

$$(-\zeta_{2p})^p = (-1)^p (\zeta_{2p})^p = (-1)(-1) = 1.$$

If $\text{Char}(F) = p$, then $-\zeta_{2p} = 1 = \zeta_p$, but this is not the case. If $\text{Char}(F) \neq p$, then $-\zeta_{2p} \neq 1$. So, $\text{ord}(-\zeta_{2p}) = p$. Now we have shown that $-\zeta_{2p}$ is a primitive p -th root of unity for every odd prime p .

Now assume (3) holds and $\zeta_{2p} \in E \setminus F$, for some $p \in \mathbb{P}$. Then p should be an odd prime, otherwise we would have that $p = 2$. So, we have $\zeta_4 \in E \setminus F$, but this contradicts (3). If $\text{Char}(F) = 2$, then $\zeta_{2p} = \zeta_p \in E \setminus F$, but this contradicts (3). If $\text{Char}(F) \neq 2$, then we have $-\zeta_{2p} = \zeta_p \in E \setminus F$. Again this contradicts (3). So we have shown (3) \implies (4).

(4) \implies (3) : Conversely assume that (4) holds. For $p = 2$, we have $\zeta_4 \notin E \setminus F$, and (3) follows. Now suppose that p is an odd prime and $\zeta_p \in E$. We have to show that $\zeta_p \in F$. Suppose that $\zeta_p \notin F$. Then we have $\pm\zeta_{2p} \in E$, using the facts above. But assuming that $\zeta_p \notin F$, we have $\pm\zeta_{2p} \notin F$. So, $\zeta_{2p} \in E \setminus F$, and this contradicts (4). Thus we have proven (4) \implies (3). Hence we are done. \square

Remarks 3.4.3. (1) A field F is said to be a *field with few n -th roots of unity*, where $n \in \mathbb{N}^*$, if $\mu_n(F) \subseteq \{-1, 1\}$, for all $n \in \mathbb{N}^*$, that is, $\mu(F) \subseteq \{-1, 1\}$. According to the definition of a pure extension, for any extension E/F with E , a field with few roots of unity, is a pure extension. Since any subfield of \mathbb{R} is a field with few roots of unity, we can say that any extension E/F , where E is a subfield of \mathbb{R} , is a pure extension.

Clearly, any extension E/F with $\mu_n(E) \subseteq F$, for all $n \in \mathbb{N}^*$, is a pure extension. Now our aim is to show that for any field F and any $m \in \mathbb{N}^*$, the extension $F(X_1, X_2, \dots, X_m)/F$ is pure. First of all we show that

$$\mu_n(F(X_1, X_2, \dots, X_m)) = \mu_n(F), \quad (3.4.1)$$

for any field F and any $m, n \in \mathbb{N}^*$. Then we can deduce that $F(X_1, X_2, \dots, X_m)/F$ is a pure extension by the Equation (3.4.1) and the fact that $\mu_n(F) \subseteq F$. Clearly,

$$\mu_n(F) \subseteq \mu_n(F(X_1, X_2, \dots, X_m)).$$

Now we show the other inclusion.

Let $f/g \in \mu_n(F(X_1, X_2, \dots, X_m))$, we have $(f/g)^n = 1$, and $f, g \in F[X_1, X_2, \dots, X_m]$. Since $f^n = g^n$, we have that the irreducible factors of f and g are the same. Now we put $f = a \cdot p_1^{k_1} \dots p_s^{k_s}$ and $g = b \cdot p_1^{l_1} \dots p_s^{l_s}$, where $a, b \in F^*$ and $s, l_i, k_i \in \mathbb{N}^*$, and p_i are irreducible polynomials over F , for all $i \in \{1, 2, \dots, s\}$. Since $f^n = g^n$, we have $a^n = b^n$ and $l_i = k_i$, for all $1 \leq i \leq s$. So, $f/g = a/b$. But $a^n = b^n$, so $(a/b)^n = 1$, and we have $f/g \in \mu_n(F)$. Therefore,

$$\mu_n(F(X_1, X_2, \dots, X_m)) = \mu_n(F).$$

This implies that $F(X_1, X_2, \dots, X_m)/F$ is a pure extension. In particular the extension $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$ is also pure.

(2) A quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where d is a square-free integer is pure if and only if $d \neq -1, -3$. We will see this in Corollary 3.4.16. \square

Proposition 3.4.4. *Let $F \subseteq K \subseteq E$ be a tower of fields. Then E/F is pure if and only if both K/F and E/K are pure.*

Proof. Clearly, we have $\mu_p(F) \subseteq \mu_p(K) \subseteq \mu_p(E)$, for every $p \in \mathcal{P}$. If E/F is a pure extension, then by Lemma 3.4.2, we have $\mu_p(E) = \mu_p(F)$, and so $\mu_p(F) = \mu_p(K) = \mu_p(E)$. Thus, K/F and E/K are both pure extensions, by Lemma 3.4.2. The other part is similar. Hence, we are done. \square

Lemma 3.4.5. *Let E/F be a finite separable G -radical extension. If E/F is pure, then E/F is G -Kneser and $G = T(E/F)$.*

Proof. Since E/F is a G -radical extension, $E = F(G)$, where $F^* \leq G \leq T(E/F)$. Then $E = F(G) \subseteq F(T(E/F))$. So, $E = F(T(E/F))$, and this implies that E/F is also a $T(E/F)$ -radical extension. Now we want to show that E/F is $T(E/F)$ -Kneser, and we are going to use The Kneser Criterion.

Let p be an odd prime such that $\zeta_p \in T(E/F)$. Then, $\zeta_p \in E$, but this implies that $\zeta_p \in F$ by Lemma 3.4.2. Now if $1 \pm \zeta_4 \in T(E/F)$, then clearly $1 \pm \zeta_4 \in E$. But this implies that $\zeta_4 \in E$. So, again by Lemma 3.4.2, we deduce that $\zeta_4 \in F$. By Theorem 3.3.12, we obtain that E/F is a $T(E/F)$ -Kneser extension. Also, by the same argument, we have that E/F is a G -Kneser extension. We have

$$T(E/F) = E \cap T(E/F) = F(G) \cap T(E/F) = G,$$

by Proposition 3.3.10. Hence we have $G = T(E/F)$, and E/F is G -Kneser. \square

Now we are going to prove the Greither-Harrison Criterion. Before this theorem, we recall the definition of a Cogalois extension. A finite extension E/F is said to be Cogalois, if E/F is a radical extension such that $|\text{Cog}(E/F)| = [E : F]$.

Theorem 3.4.6. *(The Greither-Harrison Criterion) The following statements are equivalent for a finite extension E/F .*

(1) E/F is Cogalois.

(2) E/F is radical, separable and pure.

Proof. (1) \implies (2) : Suppose that E/F is Cogalois . So it is radical. Now we show that E/F is separable extension. Suppose that E/F is not separable, so we necessarily have $\text{Char}(F) = p > 0$. Because E/F being a finite extension, it is algebraic, and we know that any algebraic extension over a field of characteristic 0 is separable.

Now p divides $[E : F]$, since in the first part of the thesis, we have seen that a power of the characteristic divides the degree of the extension. Since we have a Cogalois extension, we have

$$|\text{Cog}(E/F)| = [E/F].$$

Then p divides the order of the Cogalois group of the extension E/F . By Lemma 3.2.8 there exists an element $\widehat{\lambda} \in \text{Cog}(E/F) = T(E/F)/F^*$, of order p . So we have $\lambda^p \in F^*$, and $\lambda \notin F^*$.

Clearly F is an infinite field, otherwise E/F would be separable since any algebraic extension over a finite field is separable.

Since $\lambda \notin F$, for any $\mu \in F$, we have $\mu + \lambda \notin F$. We also have $(\mu + \lambda)^p = \mu^p + \lambda^p \in F$, since $\text{Char}(F) = p$. So, $\widehat{\mu + \lambda} \in \text{Cog}(E/F)$. Now our aim is to show that for every $\mu_1, \mu_2 \in F$ distinct, we should have

$$\widehat{\mu_1 + \lambda} \neq \widehat{\mu_2 + \lambda}.$$

If we have $\widehat{\mu_1 + \lambda} = \widehat{\mu_2 + \lambda}$, then $\mu_1 + \lambda = a(\mu_2 + \lambda)$, for some $a \in F^*$. If $a \neq 1$, then $\mu_1 - a\mu_2 = \lambda(a - 1)$. But we can multiply both sides of this equation by the inverse of $a - 1$ (inverse of $a - 1$ exists, since $a - 1$ is not equal to 0). Hence,

$$\lambda = (\mu_1 - a\mu_2)(a - 1)^{-1}. \quad (3.4.2)$$

But the right hand side of Equation (3.4.2) lies in F , so λ should be in F . But this is a contradiction. Thus, $a = 1$, and this means that $\mu_1 + \lambda = \mu_2 + \lambda$. Hence, $\mu_1 = \mu_2$.

Therefore we have shown that for every $\mu_1, \mu_2 \in F$ distinct, $\widehat{\mu_1 + \lambda} \neq \widehat{\mu_2 + \lambda}$. But we know that F is an infinite field, so according to what we have shown above, we can say that $\text{Cog}(E/F)$, which is finite, contains infinitely many elements of the form $\widehat{\mu + \lambda}$, where $\mu \in F$. But this is a contradiction. Hence we have shown that E/F is a separable extension.

Now it remains to show that E/F is a pure extension. We prove this by using Lemma 3.4.2. Suppose that $\zeta \in \mu_q(E)$, so, $\zeta^q = 1$. We claim that $\zeta \in F$.

Let q be an odd prime. If $\text{Char}(F) = p = q$, then $\zeta^p = \zeta^q = 1$, that is, $\zeta = 1 \in F$. So we may suppose that $q \neq p = \text{Char}(F)$. And we can take $\zeta \neq 1$, since $1 \in F$. Then we have

$$1 + \zeta + \zeta^2 + \dots + \zeta^{q-1} = 0,$$

since $\zeta \neq 1$ is a root of the polynomial $X^q - 1 \in F[X]$. This implies that $1, \zeta, \zeta^2, \dots, \zeta^{q-1}$ are linearly dependent over F .

Clearly, $\widehat{\zeta} \in \text{Cog}(E/F) = t(E^*/F^*)$, since $\widehat{\zeta}^q = \widehat{1}$. Then $\text{ord}(\widehat{\zeta})$ in $\text{Cog}(E/F)$ is either 1 or q . If $\text{ord}(\widehat{\zeta}) = q$, then the elements $\widehat{1}, \widehat{\zeta}, \widehat{\zeta}^2, \dots, \widehat{\zeta}^{q-1}$ of $\text{Cog}(E/F)$ are distinct. So, by Corollary 3.3.9, we obtain that $1, \zeta, \zeta^2, \dots, \zeta^{q-1} \in E$ are linearly independent over F . But this is contradiction, hence $\text{ord}(\widehat{\zeta}) = 1$ in $\text{Cog}(E/F)$, that is $\zeta \in F^*$.

Now we investigate the case $q = 4$. By the same reasoning, we may suppose that $\text{Char}(F) \neq 2$. Since we have

$$1 + \zeta - (1 + \zeta) = 0,$$

the elements $1, \zeta, 1 + \zeta$ of E are linearly dependent over F . So, again by Corollary 3.3.9, we have that $\widehat{1}, \widehat{\zeta}, \widehat{1 + \zeta} \in \text{Cog}(E/F)$ can not be distinct. But any equality gives that $\zeta \in F$. Hence, the extension E/F is pure by Lemma 3.4.2.

Conversely, suppose that the extension E/F is radical, separable and pure. By Lemma 3.4.5, we have that E/F is $T(E/F)$ -Kneser. By Corollary 3.3.9, this implies that

$$|T(E/F)/F^*| = |\text{Cog}(E/F)| = [E : F].$$

And this implies that E/F is a Cogalois extension. Hence we are done. \square

Examples 3.4.7. (1) The quartic extension $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is separable, since it is algebraic over a field of characteristic 0. It is algebraic since it is a finite extension. Since we have shown that any extension E/F , where E is a subfield of \mathbb{R} is pure, we deduce that the extension $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is pure, since $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is a subfield of \mathbb{R} . But in Proposition 3.4.13, we will show that the extension $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is neither radical, nor Cogalois.

(2) The quadratic extension $\mathbb{Q}(i)/\mathbb{Q}$ is separable, since it is an algebraic extension over a field of characteristic 0. Also, $\mathbb{Q}(i)/\mathbb{Q}$ is clearly a G -radical extension, where $G = \mathbb{Q}^* \langle i \rangle$ and $\mathbb{Q}^* \leq G \leq T(\mathbb{Q}(i)/\mathbb{Q})$. But $\mathbb{Q}(i)/\mathbb{Q}$ is not a pure extension since $\mu_p(\mathbb{Q}(i)) \subseteq \mathbb{Q}$ does not hold for all $p \in \mathcal{P}$. Consider $p = 3 \in \mathcal{P}$. The primitive third root of unity is clearly in $\mu_3(\mathbb{Q}(i))$, but it is not contained in \mathbb{Q} . Hence, the extension $\mathbb{Q}(i)/\mathbb{Q}$ is not pure. So, from Theorem 3.4.6, we deduce that $\mathbb{Q}(i)/\mathbb{Q}$ is not a Cogalois extension. In Proposition 3.4.15 (2) we will see that

$$\text{Cog}(\mathbb{Q}(i)/\mathbb{Q}) = \{\widehat{1}, \widehat{i}, \widehat{1+i}, \widehat{1-i}\} = \langle 1+i \rangle \cong \mathbb{Z}_4.$$

(3) The quadratic extension $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$ is G -radical, where $G = \mathbb{F}_2^*(X^2) \langle X \rangle$. Also this extension is pure by Remarks 3.4.3. But it is not separable. Let $E = \mathbb{F}_2(X)$ and $F = \mathbb{F}_2(X^2)$. Now our aim is to show that E/F is not separable. Let $X = u$. Then $F(u) = \mathbb{F}_2(X^2)(X) \subseteq E$. We also have

$$E = \mathbb{F}_2(X) \subseteq \mathbb{F}_2(X)(X^2) = \mathbb{F}_2(X^2)(X) = F(u).$$

So, $E = F(u)$.

Now we claim that $\text{Min}(u, F) = Z^2 - u^2$. Clearly, u is a root of $Z^2 - u^2$. Suppose that $Z^2 - u^2$ is reducible over F . Then it would have a root in F . But the roots of this polynomial are u and $-u$ which do not belong to F . Hence, $Z^2 - u^2$ is irreducible over F . So, $\text{Min}(u, F) = Z^2 - u^2$. But $(Z^2 - u^2)' = 0$, so E/F is not separable. So, it is not Cogalois. \square

Theorem 3.4.8. (*The Gay-Vélez Criterion*) *The following assertions are equivalent for a finite extension E/F .*

- (1) E/F is Cogalois.
- (2) E/F is radical, separable, and satisfies the following conditions: for every odd prime p , $\zeta_p \in F$ whenever $\zeta_p \in T(E/F)$, and $\zeta_4 \in F$ whenever $1 \pm \zeta_4 \in T(E/F)$.
- (3) E/F is radical, separable, and $\zeta_{2p} \notin E \setminus F$ for every $p \in \mathbb{P}$.

Proof. (1) \iff (3) follows from Lemma 3.4.2 and Theorem 3.4.6.

(1) \implies (2) : Suppose that E/F is a Cogalois extension. By Remarks 3.3.11 we know that E/F is a $T(E/F)$ -Kneser extension. If we apply Kneser Criterion to this extension where $G = T(E/F)$, we obtain (2).

(2) \implies (1) : By Kneser Criterion, we deduce that E/F is $T(E/F)$ -Kneser, so it is a Cogalois extension. Hence we are done. \square

Remark 3.4.9. By The Greither-Harrison Criterion, it follows that any Cogalois extension is separable. On the other hand a Kneser extension does not have to be a separable extension. Consider $\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$. This extension is not separable by (3) of Examples 3.4.7. But, it is a Kneser extension. Let $E = \mathbb{F}_2(X)$ and $F = \mathbb{F}_2(X^2)$. We take $G = F^*\langle X \rangle$. Now our aim is to show that E/F is G -Kneser. By Examples 3.4.7 (3) we have $E = F(u)$, where $u = X$, and $\text{Min}(u, F) = Z^2 - u^2$. Therefore,

$$[E : F] = [F(u) : F] = 2.$$

If we show that the order of \widehat{X} is 2 in $F^*\langle X \rangle/F^*$, then we are done, since we have $|G/F^*| = |F^*\langle X \rangle/F^*| = \text{ord}(\widehat{X})$. But $\widehat{X} = XF^*$, and clearly, $(XF^*)^2 \in F^*$. Thus,

$$|G/F^*| = |F^*\langle X \rangle/F^*| = \text{ord}(\widehat{X}) = 2 = [E : F].$$

Therefore, E/F is G -Kneser. \square

3.4.2 Some Examples and Properties of Cogalois Extensions

In this section we present some examples concerning Cogalois extensions Also we list some basic properties of Cogalois extensions.

Examples 3.4.10. (1) We have seen in Remarks 3.4.3 that the extension E/F is pure, where E is a subfield of \mathbb{R} . So any finite G -radical extension E/F with E a subfield of \mathbb{R} is Cogalois by Greither-Harrison Criterion. It is clear that E/F is separable. Because $\mathbb{Q} \subseteq F \subseteq E$ and E/F being finite, it is algebraic. And E is an algebraic extension over a field of characteristic 0. So, E/F is separable.

Now by Lemma 3.4.5, we have $G = T(E/F)$. But this implies that

$$\text{Cog}(E/F) = T(E/F)/F^* = G/F^*.$$

Now consider the extension

$$\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q},$$

with $r \in \mathbb{N}^*$, $a_1, \dots, a_r, n_1, \dots, n_r \in \mathbb{N}^*$ and $\sqrt[n_i]{a_i}$ is a positive real n_i -th root of a_i , for all i , $1 \leq i \leq r$. Using the same idea as above, we deduce that this extension is a G -radical Cogalois extension, where $G = \mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle$. Hence the Cogalois group of this extension is $\mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle / \mathbb{Q}^*$.

(2) A quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where $d \neq 1$ is a square free integer, is Cogalois if and only if $d \neq -1, -3$. This will be shown at the end of this section.

(3) We know that $\mathbb{Q}(\zeta_9, \sqrt[9]{5})$ is a splitting field of the separable polynomial

$$f = X^9 - 5 \in \mathbb{Q}[X],$$

where roots of f are $\zeta_9^i \sqrt[9]{5}$, $0 \leq i \leq 8$. So, $\mathbb{Q}(\zeta_9, \sqrt[9]{5})$ is a Galois extension by Proposition 2.6.7. Hence, $\mathbb{Q}(\zeta_9, \sqrt[9]{5})/\mathbb{Q}(\zeta_3)$ is a Galois extension. Also this extension is Cogalois. Clearly, it is separable and G -radical, where $G = (\mathbb{Q}(\zeta_3))^* \langle \zeta_9, \sqrt[9]{5} \rangle$. \square

Proposition 3.4.11. *The following assertions hold for a tower of fields $F \subseteq K \subseteq E$.*

(1) *There exists a canonical exact sequence of Abelian groups.*

$$1 \longrightarrow \text{Cog}(K/F) \longrightarrow \text{Cog}(E/F) \longrightarrow \text{Cog}(E/K).$$

(2) *If E/F is a Cogalois extension, then E/K and K/F are both Cogalois extensions.*

- (3) If E/F is a radical extension, and E/K , K/F are both Cogalois extensions, then E/F is a Cogalois extension.
- (4) If E/F is Cogalois, then the groups $\text{Cog}(E/K)$ and $\text{Cog}(E/F)/\text{Cog}(K/F)$ are canonically isomorphic.

Proof. (1) We claim that the canonical map

$$\text{Cog}(E/F) \longrightarrow \text{Cog}(E/K), \quad xF^* \longmapsto xK^*$$

is a group homomorphism with kernel $\text{Cog}(K/F)$. It is clear that this map is a homomorphism. Now we show that the kernel of this homomorphism is $\text{Cog}(K/F)$. Let x be an element of the kernel of this homomorphism. Then $xK^* = K^*$, since $\text{Cog}(E/K) = T(E/K)/K^*$. So, we have $x \in K^*$. But since

$$x \in \text{Cog}(E/F) = T(E/F)/F^*,$$

we have $x^n \in F^*$, for some $n \in \mathbb{N}^*$. But this implies that

$$x \in T(K/F)/K^* = \text{Cog}(K/F).$$

Also if $x \in \text{Cog}(K/F)$, then we can clearly see that x lies in the kernel of this homomorphism.

Now we can say that the sequence

$$\mathbf{1} \longrightarrow \text{Cog}(K/F) \longrightarrow \text{Cog}(E/F) \longrightarrow \text{Cog}(E/K),$$

of Abelian groups is exact, because the image of the first map and the kernel of the second map is $\mathbf{1}$ (the second map is the inclusion homomorphism) and also, the image of the second map and the kernel of the third map is $\text{Cog}(K/F)$, as we have shown above.

(2) Suppose that E/F is a Cogalois extension. Then, by Theorem 3.4.6, we have that E/F is radical, separable and pure. Clearly, E/K is also a radical, separable and pure extension. So, again by Theorem 3.4.6, we have that E/K is Cogalois. But

we can not easily deduce that K/F is also Cogalois, since K/F does not have to be a radical extension.

Now we are going to show that K/F is a Cogalois extension. Since E/F is a Cogalois extension, $\text{Cog}(K/F)$ is finite. Also $\text{Cog}(K/F)$ is finite, being a subgroup of $\text{Cog}(E/F)$. Now let r be the number of elements in $\text{Cog}(K/F)$. If $\widehat{x}_1, \widehat{x}_2, \dots, \widehat{x}_r$ are all the elements of $\text{Cog}(K/F) = T(K/F)/F^*$, then using Corollary 3.3.9, and the fact that E/F is Cogalois ($T(E/F)$ -Kneser), we have that the subset $\{\widehat{x}_1, \widehat{x}_2, \dots, \widehat{x}_r\}$ of K is linearly independent over F . So,

$$|\text{Cog}(K/F)| \leq [K : F].$$

From (1), we know that there exists a canonical monomorphism of groups such that

$$\text{Cog}(E/F)/\text{Cog}(K/F) \hookrightarrow \text{Cog}(E/K).$$

So, we have

$$|\text{Cog}(E/F)|/|\text{Cog}(K/F)| \leq |\text{Cog}(E/K)|,$$

since the groups $\text{Cog}(E/F)$ and $\text{Cog}(K/F)$ are finite. But we know that E/F and E/K are Cogalois extensions, so this implies that $|\text{Cog}(E/F)| = [E : F]$, and $|\text{Cog}(E/K)| = [E : K]$. Now we obtain

$$[E : F]/|\text{Cog}(K/F)| \leq [E : K] = [E : F]/[K : F].$$

But this means that

$$|\text{Cog}(K/F)| \geq [K : F].$$

Since we have the opposite inequality above, we deduce that

$$|\text{Cog}(K/F)| = [K : F].$$

From the above fact, we can say that $\{x_1, x_2, \dots, x_r\}$ is a vector space basis of K over F . So, we can write $K = F(x_1, x_2, \dots, x_r)$. Since $\text{Cog}(K/F) = T(K/F)/F^*$, we have $\{x_1, x_2, \dots, x_r\} \subseteq T(K/F)$. Thus, we have that K/F is a radical extension. Also, we

know that K/F is separable and pure. Therefore, K/F is a Cogalois extension by Theorem 3.4.6.

(3) Suppose that E/K and K/F are Cogalois extensions. Then these extensions are separable and pure by Theorem 3.4.6. But this implies that E/F is a separable extension. By Proposition 3.4.4, we also have that E/F is a pure extension. Hence by Theorem 3.4.6, we have that E/F is Cogalois, since E/F was given to be a radical extension.

(4) From (1) we know that there is a canonical monomorphism

$$\psi : \text{Cog}(E/F)/\text{Cog}(K/F) \hookrightarrow \text{Cog}(E/K)$$

of Abelian groups. From (1) we also know that E/F , E/K and K/F are all Cogalois extensions. Hence, we have $|\text{Cog}(E/F)| = [E : F]$, $|\text{Cog}(E/K)| = [E : K]$ and $|\text{Cog}(K/F)| = [K : F]$. So, we obtain

$$\begin{aligned} |\text{Cog}(E/F)/\text{Cog}(K/F)| &= |\text{Cog}(E/F)|/|\text{Cog}(K/F)| = [E : F]/[K : F] \\ &= [E : K] = |\text{Cog}(E/K)|. \end{aligned}$$

This shows that ψ surjective. But we know that ψ is a monomorphism, so ψ is an isomorphism of groups.

□

Now we give a result which says that any Cogalois extension is an extension with Cogalois correspondence.

Theorem 3.4.12. *The following statements hold for a finite Cogalois extension E/F .*

- (1) *The maps $\cap T(E/F) : \xi \longrightarrow \mathcal{C}$ and $F(-) : \mathcal{C} \longrightarrow \xi$ are isomorphisms of lattices, inverse to one another, where $\xi = \{K \mid F \subseteq K, K \text{ is a subfield of } E\}$ and*

$$\mathcal{C} = \{H \mid F^* \leq H \leq T(E/F)\}.$$
- (2) *For every intermediate field $K \in \xi$, one has $K = F(T(K/F))$.*

(3) For every subgroup $H \in \mathcal{C}$, one has $\text{Cog}(F(H)/F) = H/F^*$.

Proof. (1) Let $H \in \mathcal{C}$. Then by Proposition 3.3.10,

$$F(H) \cap T(E/F) = H.$$

Now let $K \in \xi$. Since E/F is a Cogalois extension, we have that E/K and K/F are also Cogalois extensions by the previous proposition. So, E/K is $T(E/K)$ -Kneser and E/F is $T(E/F)$ -Kneser. Then we have

$$E = F(T(E/F)) \subseteq K(T(E/F)) \subseteq K(T(E/F)K^*) \subseteq E.$$

So, $E = K(T(E/F)K^*)$. Thus, E/K is $T(E/F)K^*$ -radical, since clearly,

$$T(E/F)K^* \leq T(E/K).$$

But by Lemma 3.4.5, $T(E/F)K^* = T(E/K)$, that is E/K is $T(E/F)K^*$ -Kneser. So,

$$[E : K] = |(T(E/F)K^*)/K^*| = |T(E/F)/(K^* \cap T(E/F))|,$$

clearly, $(T(E/F)K^*)/K^*$ and $T(E/F)/(K^* \cap T(E/F))$ are group isomorphic. Hence,

$$[K : F] = [E : F]/[E : K] = |T(E/F)/F^*|/|T(E/F)/(K^* \cap T(E/F))| = |(K \cap T(E/F))/F^*|.$$

On the other hand, by Corollary 3.3.9, we have $F(K^* \cap T(E/F))/F$ is $K^* \cap T(E/F)$ -Kneser. So, we have $[F(K^* \cap T(E/F)) : F] = |K^* \cap T(E/F)/F^*|$. Since

$$F(K^* \cap T(E/F)) \subseteq F(K^*) \subseteq K(K^*) = K,$$

we deduce that $K = F(K^* \cap T(E/F))$. We also have

$$K = F(K^* \cap T(E/F)) = F(K \cap T(E/F)).$$

Hence, we have shown that these two maps given above are isomorphism of lattices, inverse to one another, since $K \in \xi$, $H \in \mathcal{C}$ are arbitrary.

(2) Let $K \in \xi$. Clearly, we have $K \cap T(E/F) = T(K/F)$. Then, we should have

$$F(T(K/F)) = K,$$

since (1) implies that the above maps are inverse to one another.

(3) Let $H \in \mathcal{C}$. We know that $H = F(H) \cap T(E/F) = T(F(H)/F)$, by Proposition 3.3.10. So, $\text{Cog}(F(H)/F) = T(F(H)/F)/F^* = H/F^*$. \square

Now we give an example which shows that the property of being radical, Kneser, or Cogalois is not transitive. We investigate the quartic extension $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$.

Proposition 3.4.13. *The following assertions hold.*

- (a) $\mathbb{Q}(\sqrt{2})$ is a subfield of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$.
- (b) $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}(\sqrt{2})] = 2$, and $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4$.
- (c) $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is not a Cogalois extension.
- (d) $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are Cogalois extensions.
- (e) (c) $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is neither a radical, nor a Kneser extension, nor a Cogalois extension.

(f) $\text{Cog}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}) = \{\widehat{1}, \widehat{\sqrt{2}}\}$.

(g) The element $\widehat{\sqrt{1+\sqrt{2}}}$ of the group $\mathbb{Q}(\sqrt{1+\sqrt{2}})^*/\mathbb{Q}^*$ has infinite order.

Proof. Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\sqrt{1+\sqrt{2}})$ and $\theta = \sqrt{1+\sqrt{2}}$.

(a) Since $\sqrt{2} = \theta^2 - 1 \in \mathbb{Q}(\theta) = E$, we have $K = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\theta) = E$. Also we have $E = K(\theta)$, since $K(\theta) = \mathbb{Q}(\sqrt{2})(\theta) = \mathbb{Q}(\theta)(\sqrt{2}) = E(\sqrt{2}) = E$. So, it is clear that K is a subfield of E .

(b) We know that θ satisfies the polynomial $f = X^4 - 2X^2 - 1$. Consider $f(X+1)$. But, we can apply the Eisenstein Criterion to $f(X+1) = X^4 + 4X^3 + 4X^2 - 2$. So, $f(X+1)$ is irreducible over \mathbb{Q} . Hence, f is irreducible over \mathbb{Q} . Hence, $[E : F] = 4$. So, $[E : K] = 2$.

(c) The conjugates of θ over \mathbb{Q} are the roots of its minimal polynomial $X^4 - 2X^2 - 1$. Since two of the roots of this polynomial are $\sqrt{1+\sqrt{2}}$, and $-\sqrt{1+\sqrt{2}}$, the other two roots of it should satisfy the equation $X^2 = 1 - \sqrt{2}$. So, clearly they are complex, and they do not belong $E \subseteq \mathbb{R}$. Therefore, E/F is not a normal extension, this means that E/F is not Galois.

(d) By Remarks 3.4.3, we know that E/F and K/F are pure extensions since E is a subfield of \mathbb{R} . Also, these extensions are separable, since they are algebraic

extensions over a field of characteristic 0. We also have $E = K(\theta) = K(K^*\langle\theta\rangle)$, and $K = F(F^*\langle\sqrt{2}\rangle)$, where $K^* \leq K^*\langle\theta\rangle \leq T(E/K)$, and $F^* \leq F^*\langle\sqrt{2}\rangle \leq T(K/F)$. So, E/K and K/F are Cogalois extensions by the Greither-Harrison Criterion.

(e) We know again by Remarks 3.4.3 that E/F is a pure extension. Also it is separable by the same reasoning as above. So, by the Greither-Harrison Criterion it is Cogalois if and only if it is radical. Since any Kneser extension is radical, if we show that E/F is not a Cogalois extension, then we can deduce that (e) holds. Now suppose that E/F is a Cogalois extension. Then we should have $[E : F] = |\text{Cog}(E/F)| = 4$. Hence this group should be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or to \mathbb{Z}_4 .

Case I: Suppose that $\text{Cog}(E/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. So, there exists some $\beta, \gamma \in \mathbb{Q}_+^*$ such that

$$\text{Cog}(E/F) = \mathbb{Q}^*\langle\sqrt{\beta}, \sqrt{\gamma}\rangle/\mathbb{Q}^* = \{\widehat{1}, \widehat{\sqrt{\beta}}, \widehat{\sqrt{\gamma}}, \widehat{\sqrt{\beta\gamma}}\}.$$

So by Corollary 3.3.9, we can see that $\{1, \sqrt{\beta}, \sqrt{\gamma}, \sqrt{\beta\gamma}\}$ is a vector space basis of E over F . Hence,

$$E = \mathbb{Q}\left(\sqrt{1 + \sqrt{2}}\right) = \mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma}).$$

But $\mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma})/\mathbb{Q}$ is a Galois extension, since it is a splitting field of the separable polynomial $(X^2 - \beta)(X^2 - \gamma)$. On the other hand, we know by (c) that $\mathbb{Q}(\sqrt{1 + \sqrt{2}})/\mathbb{Q}$ is not a Galois extension. Thus, this case is impossible.

Case II: Suppose that $\text{Cog}(E/F) \cong \mathbb{Z}_4$. Then, there exists $\alpha \in \mathbb{Q}_+^*$ such that

$$\text{Cog}(E/F) = \mathbb{Q}^*\langle\sqrt[4]{\alpha}\rangle/\mathbb{Q}^* = \{\widehat{1}, \widehat{\sqrt[4]{\alpha}}, \widehat{\sqrt[4]{\alpha^2}}, \widehat{\sqrt[4]{\alpha^3}}\}.$$

Again by Corollary 3.3.9, $\{1, \sqrt[4]{\alpha}, \sqrt[4]{\alpha^2}, \sqrt[4]{\alpha^3}\}$ is a vector space basis of E over \mathbb{Q} . So, we have

$$E = \mathbb{Q}\left(\sqrt{1 + \sqrt{2}}\right) = \mathbb{Q}(\sqrt[4]{\alpha}).$$

We can easily see that the degree of the extension $E/\mathbb{Q}(\sqrt{\alpha})$ is 2, since the minimal polynomial of $\sqrt[4]{\alpha}$ over $\mathbb{Q}(\sqrt{\alpha})$ is $X^2 - \sqrt{\alpha}$. But $[E : F] = 4$, so $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = 2$. Hence, $\sqrt{\alpha} \notin \mathbb{Q}$. Since $|\text{Cog}(E/F)| = 4$, $\text{Cog}(E/F)$ has a unique proper subgroup which has order 2. So by Theorem 3.4.12 (1), we deduce that E/F has a unique

proper intermediate field. By (a), we know that $\mathbb{Q}(\sqrt{2})$ is such an intermediate field. So we have $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{\alpha})$. Hence, $\sqrt{2} = k\sqrt{\alpha}$, where $k \in \mathbb{Q}_+^*$. Then we obtain $2 = \alpha k^2$. Since $E = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[4]{\alpha})$, there exists some $a, b, c, d \in \mathbb{Q}$ such that

$$\theta = \sqrt{1 + \sqrt{2}} = a + b\sqrt[4]{\alpha} + c\sqrt[4]{\alpha^2} + d\sqrt[4]{\alpha^3}.$$

We can write the above equation as

$$\theta - (a + c\sqrt{\alpha}) = \sqrt[4]{\alpha} (b + d\sqrt{\alpha}). \quad (3.4.3)$$

If we square the both sides of Equation (3.4.3), then we obtain

$$\theta^2 - 2\theta(a + c\sqrt{\alpha}) + (a + c\sqrt{\alpha})^2 = \sqrt{\alpha} (b + d\sqrt{\alpha})^2.$$

Clearly, $\theta^2 = 1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{\alpha})$. Since $(a + c\sqrt{\alpha})^2$ and the right hand side of the above equation are in $\mathbb{Q}(\sqrt{\alpha})$, we have that $a + c\sqrt{\alpha} = 0$. Otherwise we would have that $\theta \in \mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{2})$. But this will imply that $E = \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt{2})$. This is a contradiction, since E/K has degree 2 by (b). So we obtain

$$\theta = \sqrt[4]{\alpha} (b + d\sqrt{\alpha}). \quad (3.4.4)$$

We can write the above equation as

$$\frac{b + d\sqrt{2}}{\theta} = \frac{1}{\sqrt[4]{\alpha}},$$

but we know that $\sqrt{\alpha} = \sqrt{2}/k$, so we obtain

$$\frac{bk + d\sqrt{2}}{\theta} = \frac{k}{\sqrt[4]{\alpha}}.$$

So we deduce that $(\frac{bk+d\sqrt{2}}{\theta})^4 \in \mathbb{Q}$. Now we put

$$u := \frac{(bk + d\sqrt{2})^4}{(1 + \sqrt{2})^2} \in \mathbb{Q}.$$

Then clearly, u coincides with its conjugate in the quadratic extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Since any \mathbb{Q} -homomorphism fixes elements of \mathbb{Q} pointwise. So, we have

$$\frac{(bk + d\sqrt{2})^4}{(1 + \sqrt{2})^2} = \frac{(bk - d\sqrt{2})^4}{(1 - \sqrt{2})^2}.$$

Taking the square roots of both sides, we obtain

$$\frac{(bk + d\sqrt{2})^2}{(1 + \sqrt{2})} = \frac{(bk - d\sqrt{2})^2}{(\sqrt{2} - 1)},$$

hence,

$$(bk + d\sqrt{2})^2(\sqrt{2} - 1) = (bk - d\sqrt{2})^2(\sqrt{2} + 1).$$

So, we obtain

$$b^2k^2 - 4bdk + 2d^2 = 0.$$

We can also write the above equation as

$$(bk - 2d)^2 = 2d^2.$$

Now we claim that $d = 0$, for otherwise taking the square root of the above equation we would have $\sqrt{2} \in \mathbb{Q}$, which is a contradiction. Hence $d = 0$, so $bk = 0$. Then $b = 0$, so by Equation (3.4.3), we have $\theta = 0$, which is a contradiction. Therefore, we have proven the fact that E/F is not a Cogalois extension.

(f) Clearly,

$$\{\widehat{1}, \widehat{\sqrt{2}}\} \subseteq \text{Cog}(\mathbb{Q}(\sqrt{1 + \sqrt{2}})/\mathbb{Q}).$$

To show the other inclusion, it is enough to show that $|\text{Cog}(E/F)| = 2$. By Proposition 3.4.11, we know that there exists a canonical monomorphism of groups

$$\text{Cog}(E/F)/\text{Cog}(K/F) \hookrightarrow \text{Cog}(E/K).$$

By (d), the quadratic extensions E/K and K/F are both Cogalois. So we have

$$|\text{Cog}(E/K)| = |\text{Cog}(K/F)| = 2.$$

Then we should have $|\text{Cog}(E/F)|$ is 2 or 4. Assume that $|\text{Cog}(E/F)| = 4$. Then as in the proof of (e), there are 2 cases: $\text{Cog}(E/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\text{Cog}(E/F) \cong \mathbb{Z}_4$. In the first case, there exists $\beta, \gamma \in \mathbb{Q}_+^*$ such that

$$\text{Cog}(E/F) = \mathbb{Q}^*\langle\sqrt{\beta}, \sqrt{\gamma}\rangle/\mathbb{Q}^* = \{\widehat{1}, \widehat{\sqrt{\beta}}, \widehat{\sqrt{\gamma}}, \widehat{\sqrt{\beta\gamma}}\}.$$

Now we claim that $\{1, \sqrt{\beta}, \sqrt{\gamma}, \sqrt{\beta\gamma}\}$ is a vector space basis of E over F . We have $\sqrt{\gamma} \notin \mathbb{Q}(\sqrt{\beta})$, for otherwise there exists some $a, b \in \mathbb{Q}$ such that $\sqrt{\gamma} = a + b\sqrt{\beta}$. Squaring both sides, we obtain $\gamma = a^2 + b^2\beta + 2ab\sqrt{\beta}$. But this implies that $\sqrt{\beta} \in \mathbb{Q}$ and so, $\widehat{\beta} = \widehat{1}$ which is a contradiction. So, we should have $\sqrt{\gamma} \notin \mathbb{Q}(\sqrt{\beta})$. Hence, $[\mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma}) : \mathbb{Q}] = 4$. But this implies that $E = \mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma})$. So, clearly, E/F is a radical extension. But this contradicts (e).

If we have $\text{Cog}(E/F) \cong \mathbb{Z}_4$, then there exists $\alpha \in \mathbb{Q}_+^*$ such that

$$\text{Cog}(E/F) = \mathbb{Q}^* \langle \sqrt[4]{\alpha} \rangle / \mathbb{Q}^* = \{\widehat{1}, \widehat{\sqrt[4]{\alpha}}, \widehat{\sqrt[4]{\alpha^2}}, \widehat{\sqrt[4]{\alpha^3}}\}.$$

Clearly, $\sqrt[4]{\alpha} \notin \mathbb{Q}(\sqrt{\alpha})$. Otherwise there exists some $a, b \in \mathbb{Q}$ such that $\sqrt[4]{\alpha} = a + b\sqrt{\alpha}$. Squaring both sides, we obtain $\sqrt{\alpha} = a^2 + b^2\alpha + 2ab\sqrt{\alpha}$. Then $\sqrt{\alpha}(2ab - 1) = -a^2 - b^2\alpha$. If $2ab - 1 \neq 0$, then $\sqrt{\alpha} \in \mathbb{Q}$ which is a contradiction. So, we should have $2ab - 1 = 0$. Then, $-a^2 - b^2\alpha = 0$, but this is contradiction, since $\alpha \in \mathbb{Q}_+^*$. Hence, $\sqrt[4]{\alpha} \notin \mathbb{Q}(\sqrt{\alpha})$. This implies that $\{1, \sqrt[4]{\alpha}, \sqrt[4]{\alpha^2}, \sqrt[4]{\alpha^3}\}$ is a vector space basis of E over F . Thus, E/F is a radical extension. But this contradicts (e) again. So, we have $\text{Cog}(E/F) = 2$. Thus, we have proven (f).

(g) Assume that $\text{ord}(\widehat{1 + \sqrt{2}})$ is finite, say n . Then, $(\sqrt{1 + \sqrt{2}})^n \in \mathbb{Q}_+^*$. Now we put $(\sqrt{1 + \sqrt{2}})^n = a$, where $a \in \mathbb{Q}_+^*$. Then we have $\sqrt{1 + \sqrt{2}} = \sqrt[n]{a}$. Clearly, $\mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}$ is a Cogalois extension, hence $\mathbb{Q}(\sqrt{1 + \sqrt{2}})$ is a Cogalois extension. But this contradicts (e). Thus, we have proven (g). \square

3.4.3 The Cogalois Group of a Quadratic Extension

In general, to calculate the Cogalois group of a given extension is quite hard. In this subsection, we are going to give a description of the Cogalois group of any quadratic extension.

We will denote $\sqrt{-1}$ by i , and $\sqrt{-d}$ by $i\sqrt{d}$, for any $d \in \mathbb{Q}_+^*$ as usual.

Lemma 3.4.14. *Let $d \neq 1$ be a square-free rational integer, and let W denote the group of roots of unity $\mu(\mathbb{Q}(\sqrt{d}))$ in $\mathbb{Q}(\sqrt{d})$. Then*

- (1) $W = \mu_2(\mathbb{C}) = \{\pm 1\}$ if $d \neq -1, -3$.
- (2) $W = \mu_4(\mathbb{C}) = \{\pm 1, \pm i\}$ if $d = -1$.
- (3) $W = \mu_6(\mathbb{C}) = \{\pm 1, \pm(1 + i\sqrt{3})/2, \pm(1 - i\sqrt{3})/2\}$ if $d = -3$. □

Proposition 3.4.15. *Let $E = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a square-free integer. Then*

- (1) $\text{Cog}(E/\mathbb{Q}) = \langle \widehat{\sqrt{d}} \rangle \cong \mathbb{Z}_2$ if $d \neq -1, -3$.
- (2) $\text{Cog}(E/\mathbb{Q}) = \langle \widehat{1+i} \rangle \cong \mathbb{Z}_4$ if $d = -1$.
- (3) $\text{Cog}(E/\mathbb{Q}) = \langle \widehat{i\sqrt{3} \cdot (1+i\sqrt{3})} \rangle \cong \mathbb{Z}_6$ if $d = -3$.

Proof. Let $\alpha \in T(E/\mathbb{Q})$, $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$, since $\alpha \in E^* = \mathbb{Q}(\sqrt{d})^*$. We have $\text{Cog}(E/\mathbb{Q}) = T(E/\mathbb{Q})/\mathbb{Q}^*$. Now consider $\widehat{\alpha} \in \text{Cog}(E/\mathbb{Q})$. It is clear that $\widehat{\alpha} = \widehat{1}$ if and only if $\alpha \in \mathbb{Q}$.

Now suppose that $\alpha \notin \mathbb{Q}$, that is $b \neq 0$. Since $\alpha \in T(E/\mathbb{Q})$, there exists some $n \in \mathbb{N}^*$, $n > 1$ such that $\alpha^n = c \in \mathbb{Q}^*$. So α is root of $f = X^n - c \in \mathbb{Q}[X]$. The roots of this polynomial are $\alpha \xi$, where ξ is a primitive n -th root of unity. Since $E = \mathbb{Q}(\sqrt{d})$ and $\alpha = a + b\sqrt{d}$, where $a, b \in \mathbb{Q}$, we have $E = \mathbb{Q}(\alpha)$. So, the minimal polynomial $\text{Min}(\alpha, \mathbb{Q})$ of α over \mathbb{Q} has degree 2, since $[E : \mathbb{Q}] = 2$. Clearly, $\text{Min}(\alpha, \mathbb{Q})$ divides f . So the roots of $\text{Min}(\alpha, \mathbb{Q})$ are $\alpha, \alpha\xi$, where $\xi \in \mu(\mathbb{C})$. E/\mathbb{Q} is a normal extension since the minimal polynomial of each element of E splits over E . Since α and $\alpha\xi$ are conjugates elements over \mathbb{Q} , $\alpha\xi \in E$. We have $\xi = (\alpha\xi)/\alpha$, so $\xi \in E \cap \mu(\mathbb{C}) = \mu(E) = W$.

On the other hand, the product of the roots of $\text{Min}(\alpha, \mathbb{Q})$ belongs to \mathbb{Q} , i.e.,

$$\alpha^2\xi \in \mathbb{Q}. \tag{3.4.5}$$

Now we are going to deal with three cases considered in the proposition.

Case I: $d \neq -1, -3$. By the previous Lemma, we have $\xi \in \{-1, 1\}$. Then by

Equation (3.4.5), $\alpha^2 \in \mathbb{Q}$. So, $a^2 + db^2 + 2ab\sqrt{d} \in \mathbb{Q}$. Then we should have $ab = 0$. But we assumed first that $b \neq 0$, so we have $a = 0$. Thus, $\alpha = b\sqrt{d}$, and so $\widehat{\alpha} = \widehat{\sqrt{d}}$. Hence,

$$\text{Cog}(E/\mathbb{Q}) = \langle \widehat{1}, \widehat{\sqrt{d}} \rangle = \langle \widehat{\sqrt{d}} \rangle \cong \mathbb{Z}_2.$$

Case II:

$d = -1$. We have $\alpha = a + bi$ and $\alpha^2 = a^2 - b^2 + 2abi$. By the previous lemma again, $\xi \in \{1, -1, i, -i\}$.

If we have $\xi = \pm 1$, then Equation (3.4.5) implies that $\alpha^2 \in \mathbb{Q}$. So, $a^2 - b^2 + 2abi \in \mathbb{Q}$. Again we should have $ab = 0$, so $a = 0$. Thus, $\alpha = bi$, and $\widehat{\alpha} = \widehat{i}$.

If $\xi = \pm i$, then Equation (3.4.5) implies that $i\alpha^2 \in \mathbb{Q}$. So, $(a^2 - b^2)i - 2ab \in \mathbb{Q}$. Hence, $a^2 - b^2 = 0$, and so $a = \pm b$.

If we have $a = b$, then $\alpha = a + bi = b(1 + i)$. So, $\widehat{\alpha} = \widehat{1 + i}$. If $a = -b$, then $\alpha = -b(1 - i)$. Hence, $\widehat{\alpha} = \widehat{1 - i}$. Therefore,

$$\text{Cog}(\mathbb{Q}(i)/\mathbb{Q}) = \{\widehat{1}, \widehat{i}, \widehat{1 + i}, \widehat{1 - i}\} = \langle \widehat{1 + i} \rangle \cong \mathbb{Z}_4.$$

Case III: $d = -3$. We have $\alpha = a + bi\sqrt{3}$ and $\alpha^2 = a^2 - 3b^2 + 2abi\sqrt{3}$. By the previous lemma again, $\xi \in \{\pm 1, \pm(1 + i\sqrt{3})/2, \pm(1 - i\sqrt{3})/2\}$.

If $\xi = \pm 1$, then Equation (3.4.5) implies that $\alpha^2 \in \mathbb{Q}$. So, we should have that $ab = 0$. Then $a = 0$, and so $\alpha = bi\sqrt{3}$. Hence, $\widehat{\alpha} = \widehat{i\sqrt{3}}$.

If $\xi = \pm(1 + i\sqrt{3})/2$, then again by Equation (3.4.5), we have $(1 + i\sqrt{3})\alpha^2 \in \mathbb{Q}$. Thus,

$$a^2 - 3b^2 - 6ab + (a^2 - 3b^2 + 2ab)i\sqrt{3} \in \mathbb{Q}.$$

Clearly we should have that $a^2 - 3b^2 + 2ab = (a - b)(a + 3b) = 0$. So we have either $a = b$ or $a = -3b$.

If $a = b$, then $\alpha = b(1 + i\sqrt{3})$, and so $\widehat{\alpha} = \widehat{1 + i\sqrt{3}}$. If we have $a = -3b$, then $\alpha = b(-3 + i\sqrt{3})$. Hence, $\widehat{\alpha} = \widehat{-3 + i\sqrt{3}} = \widehat{i\sqrt{3}} \cdot \widehat{(1 + i\sqrt{3})}$.

If $\xi = \pm(1 - i\sqrt{3})/2$, then we have $(1 - i\sqrt{3})\alpha^2 \in \mathbb{Q}$. Thus,

$$a^2 - 3b^2 + 6ab + (-a^2 + 3b^2 + 2ab)i\sqrt{3} \in \mathbb{Q}.$$

So, we should have $-a^2 + 3b^2 + 2ab = (a + b)(-a + 3b) = 0$. So we have either $a = -b$ or $a = 3b$.

If $a = -b$, then $\alpha = -b(1 - i\sqrt{3})$, hence $\widehat{\alpha} = 1 - i\sqrt{3}$. If $a = 3b$, then we have $\alpha = b(3 + i\sqrt{3})$, and so $\widehat{\alpha} = 3 + i\sqrt{3} = i\sqrt{3} \cdot (1 - i\sqrt{3})$. Therefore,

$$\text{Cog}(E/\mathbb{Q}) = \{\widehat{1}, \widehat{i\sqrt{3}}, \widehat{1+i\sqrt{3}}, \widehat{i\sqrt{3} \cdot (1+i\sqrt{3})}, \widehat{1-i\sqrt{3}}, \widehat{i\sqrt{3} \cdot (1-i\sqrt{3})}\} \cong \mathbb{Z}_6.$$

□

Corollary 3.4.16. *The following statements are equivalent for a square-free rational integer $d \neq 1$. integer.*

- (1) $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a pure extension.
- (2) $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a Cogalois extension.
- (3) $d \neq -1, -3$.

Proof. By Proposition 3.4.15, $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a Cogalois extension if and only if we have $|\text{Cog}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})| = 2$, that is, by Proposition 2.3.15 again, if and only if $d \neq -1, -3$. So we have (2) \iff (3). The equivalence (1) \iff (2) follows from the Greither-Harrison Criterion. □

3.5 Strongly Kneser Extensions

In this chapter we are going to introduce the notions of *Cogalois connection*, *strongly G -Kneser extension* and *G -Cogalois extension*. G -Cogalois extensions are separable G -Kneser extensions E/F for which there exists a canonical lattice isomorphism between the lattice of all subextensions of E/F and the lattice of all subgroups of the group G/F^* . Also we are going to provide a characterization of G -Cogalois extensions in terms of *n -purity*.

We show that a separable G -Kneser extension E/F is G -Cogalois if and only if the group G/F^* has a prescribed structure. As a consequence, we deduce that the group G is unique. This means that if the extension E/F is simultaneously G -Cogalois and H -Cogalois, then we should have $G = H$. Then the *Kneser group* of a G -Cogalois extension can be defined as the group G/F^* , and this group will be denoted by $\text{Kne}(E/F)$.

Throughout this section, E/F will denote a fixed extension and G a group such that $F^* \leq G \leq E^*$. We also use the following notation:

$$\mathcal{G} := \{H \mid F^* \leq H \leq G\},$$

$$\xi := \underline{\text{Intermediate}}(E/F) = \{K \mid F \subseteq K, K \text{ subfield of } E\}.$$

3.5.1 Galois and Cogalois Connections

In this subsection we are going to present the dual concepts of *Galois connection* and *Cogalois connection* for arbitrary posets. The concept of *closed element* is also provided. Then, the concepts of *field extension with Galois correspondence* and *field extension with Cogalois correspondence* are introduced.

Definition 3.5.1. A Galois connection between the posets (X, \leq) and (Y, \leq) is a pair of order-reversing maps

$$\alpha : X \longrightarrow Y \text{ and } \beta : Y \longrightarrow X$$

satisfying the following conditions:

$$x \leq (\beta \circ \alpha)(x), \forall x \in X, \text{ and } y \leq (\alpha \circ \beta)(y), \forall y \in Y.$$

□

Whenever we have a Galois connection as in the above definition, we are going to use the notation

$$X \begin{array}{c} \xrightarrow{\alpha} \\ \xleftarrow{\beta} \end{array} Y.$$

If the maps α and β are both order-preserving instead of order-reversing, we obtain a *Cogalois connection* between X and Y . Now we have the following definition.

Definition 3.5.2. A Cogalois connection between the posets $(X, \leq Y)$ and $(Y, \leq Y)$ is a pair of order-preserving maps

$$\alpha : X \longrightarrow Y \text{ and } \beta : Y \longrightarrow X$$

satisfying the following conditions:

$$(\beta \circ \alpha)(x) \leq x, \forall x \in X, \text{ and } y \leq (\alpha \circ \beta)(y), \forall y \in Y.$$

□

Now if we denote by X^{op} the opposite poset of X , then clearly,

$$X \begin{array}{c} \xrightarrow{\alpha} \\ \xleftarrow{\beta} \end{array} Y$$

is a Cogalois connection if and only if

$$X^{op} \begin{array}{c} \xrightarrow{\alpha} \\ \xleftarrow{\beta} \end{array} Y$$

is a Galois connection. Now if we have

$$X \begin{array}{c} \xrightarrow{\alpha} \\ \xleftarrow{\beta} \end{array} Y$$

is a Galois connection, then

$$Y \begin{array}{c} \xrightarrow{\alpha} \\ \xleftarrow{\beta} \end{array} X$$

is also a Galois connection. But we do not have the same property for a Cogalois connection.

Let

$$X \begin{array}{c} \xrightarrow{\alpha} \\ \xleftarrow{\beta} \end{array} Y$$

be a Galois or Cogalois connection. Let $x \in X$ (resp. $y \in Y$), then the element $\alpha(x)$ (resp. $\beta(y)$) is denoted by x' (resp. y'). Now we shall use the notation:

$$x'' := (x')', \quad x''' := (x'')', \quad y'' := (y')', \quad y''' := (y'')'.$$

If we have $z'' = z$ for an element z in X or Y , then z is said to be a *closed element* of X or Y . A closed element is also called *Galois object* (resp. *Cogalois object*) in the case of a Galois (resp. Cogalois) connection. \overline{X} (resp. \overline{Y}) denotes the set of all closed elements of X (resp. Y).

The following proposition lists the basic properties of Galois and Cogalois connections.

Proposition 3.5.3. *With the notation above, the following assertions hold for a Galois or Cogalois connection between the posets X and Y .*

- (1) $z' = z'''$ for every element z of X or Y .
- (2) $\overline{X} = \beta(Y)$ and $\overline{Y} = \alpha(X)$.
- (3) The restrictions $\overline{\alpha} : \overline{X} \rightarrow \overline{Y}$ and $\overline{\beta} : \overline{Y} \rightarrow \overline{X}$ of α and β to the sets of closed elements of X and Y are bijections inverse to one another.

Proof. We will only consider the case of a Cogalois connection.

(1) Let $x \in X$ and $y \in Y$. Since $\alpha(x) = x'$ and $\beta(y) = y'$, we have $x'' \leq x$ and $y \leq y''$ by Definition 3.5.2. Since the priming operation is order-preserving in the case of a Cogalois connection, we have

$$x''' = (x'')' \leq x' \text{ and } y' \leq (y'')'.$$

Since x' is an element of Y , we have $x' \leq (x')'' = x'''$. But this proves that $x''' = x$. Since $y' \in X$, we have $(y')'' = y''' \leq y'$. Hence we obtain $y''' = y$. So we have proven (1).

(2) Let $x \in \overline{X}$. Then we have $x'' = x$. So, $x = x'' = (x')' = \beta(x') \in \beta(Y)$. Conversely, let $x \in \beta(Y)$. Then, $x = \beta(y) = y'$, for some $y \in Y$. But we have $y' = y''' = (y'')''$ by (1) and so $x = x''$. Thus, $x \in \overline{X}$. Hence, $\overline{X} = \beta(Y)$. The other equality can be proven in a similar way.

(3) Let $y \in \overline{Y}$. Then by (2), there exists some $x \in X$ such that $y = \alpha(x) = x'$. So,

$$(\overline{\alpha} \circ \overline{\beta})(y) = \alpha(\beta(\alpha(x))) = x''' = x' = y.$$

In a similar way, one can show $(\overline{\beta} \circ \overline{\alpha})(x) = x$, for all $x \in \overline{X}$. □

The most important example of a Galois connection is the one which we studied in Galois Theory. Actually, the name, Galois connection comes from there. Let E/F be an arbitrary field extension, and denote by Γ the Galois group $\text{Gal}(E/F)$ of E/F . Then clearly the maps

$$\alpha : \underline{\text{Intermediate}}(E/F) \longrightarrow \underline{\text{Subgroups}}(\Gamma), \quad \alpha(K) = \text{Gal}(E/K),$$

and

$$\beta : \underline{\text{Subgroups}}(\Gamma) \longrightarrow \underline{\text{Intermediate}}(E/F), \quad \beta(\Delta) = \text{Fix}(\Delta),$$

gives a canonical Galois connection between the lattice $\underline{\text{Intermediate}}(E/F)$ of all intermediate fields of the extension E/F and the lattice $\underline{\text{Subgroups}}(\Gamma)$ of all subgroups of Γ . We will call it the *standard Galois connection associated with the extension E/F* .

Proposition 3.5.4. *With the notation above, the following assertions are equivalent for a finite extension E/F with Galois group Γ .*

- (1) E/F is a Galois extension.
- (2) Every intermediate field of the extension E/F is a closed element in the standard Galois connection associated with E/F .
- (3) F is a closed element in the standard Galois connection associated with E/F .
- (4) The map α is injective.
- (5) The map β is surjective.
- (6) The maps α and β establish anti-isomorphism of lattices, inverse to one another, between the lattices $\underline{\text{Intermediate}}(E/F)$ and $\underline{\text{Subgroups}}(\Gamma)$.

Proof. By Part I, we can easily see that (1) \implies (2) \implies (3) \implies (1) \implies (6). Also (6) \implies (5) and (6) \implies (4) are clear.

(5) \implies (3) : Suppose that β is surjective. Then $F = \beta(\Delta) = \text{Fix}(\Delta) = \Delta'$, for some $\Delta \leq \Gamma$. So $F'' = \text{Fix}(\Delta)'' = (\Delta')'' = \Delta''' = \Delta' = \text{Fix}(\Delta) = F$. Hence, F is a closed element in the standard Galois connection associated with E/F .

(4) \implies (3) : Suppose that α is injective. We know that $F' = F''' = (F'')'$. So, $\alpha(F) = \alpha(F''')$. But since α is assumed to be injective, we have $F = F''$. Hence, F is a closed element of the extension E/F . \square

Let E/F be a G -radical extension. Then the maps

$$\chi : \underline{\text{Intermediate}}(E/F) \longrightarrow \underline{\text{Subgroups}}(G/F^*), \quad \chi(K) = (K \cap G)/F^*,$$

$$w : \underline{\text{Subgroups}}(G/F^*) \longrightarrow \underline{\text{Intermediate}}(E/F), \quad w(H/F^*) = F(H),$$

set a Cogalois connection between the lattices $\underline{\text{Intermediate}}(E/F)$ and $\underline{\text{Subgroups}}(G/F^*)$.

We call it the *standard Cogalois connection associated with the extension E/F* . It is easy to see that the standard Cogalois connection is associated with only radical extensions, whereas the standard Galois connection is associated with any extension.

Clearly, the lattice $\underline{\text{Subgroups}}(G/F^*)$ is canonically isomorphic to the lattice

$$\mathcal{G} = \{H \mid F^* \leq H \leq G\}.$$

Now we denote ξ by the lattice of all intermediate fields of the extension E/F . Then the Cogalois connection that is described above, is the same with the one which is below. Also it will be called the *standard Cogalois connection associated with E/F* :

$$\xi \begin{array}{c} \xrightarrow{\varphi} \\ \xleftarrow{\psi} \end{array} \mathcal{G}$$

where

$$\varphi : \xi \longrightarrow \mathcal{G}, \quad \varphi(K) = K \cap G,$$

$$\psi : \mathcal{G} \longrightarrow \xi, \quad \psi(H) = F(H).$$

Now we can define the following concepts.

Definition 3.5.5. *An extension E/F with Galois group Γ is said to be an extension with Γ -Galois correspondence if the standard Galois connection associated with E/F yields a lattice anti-isomorphism between the lattices $\underline{\text{Intermediate}}(E/F)$ and $\underline{\text{Subgroups}}(\Gamma)$.*

Dually, a G -radical extension E/F is said to be an extension with G/F^ -Cogalois correspondence if the standard Cogalois connection associated with E/F gives rise to a lattice isomorphism between the lattices $\underline{\text{Intermediate}}(E/F)$ and $\underline{\text{Subgroups}}(G/F^*)$.*

□

Remark 3.5.6. Clearly, by Proposition 3.5.4, any finite extension E/F with Γ -Galois correspondence is necessarily a Galois extension. Also the fact that E/F is an extension with Γ -Galois correspondence implies that $[E : F] = |\text{Gal}(E/F)|$, this follows from Proposition 2.6.7.

Conversely, if we have the equality $[E : F] = |\text{Gal}(E/F)|$ for a finite extension E/F , then E/F is necessarily a Galois extension. Let $\text{Fix}(\text{Gal}(E/F)) = L$. By Lemma 2.6.9, $[E : L] \leq |\text{Gal}(E/F)|$. Similar to the proof of Lemma 2.6.9, one can show that $[E : L] \geq |\text{Gal}(E/F)|$. So, $[E : L] = |\text{Gal}(E/F)|$. But we have $[E : L] \leq [E : F]$, since $F \subseteq L$. We have also $[E : F] = |\text{Gal}(E/F)|$. Hence, $[E : F] = [E : L]$. Therefore, $F = L$. So, E/F is a Galois extension.

But we do not have the same situation for a finite extension E/F with G/F^* -Cogalois correspondence. For such extensions, the equality $[E : F] = |G/F^*|$ which says that E/F is G -Kneser is, in general, not a consequence of the fact that E/F is an extension with G/F^* -Cogalois correspondence. \square

3.5.2 Strongly G -Kneser Extensions

A subextension of a Kneser extension is not necessarily a Kneser extension. For example, $\mathbb{Q}(\sqrt{2 + \sqrt{2}})/\mathbb{Q}$ is not a Kneser extension since it is not radical. On the other hand, we have $\mathbb{Q}(\sqrt{2 + \sqrt{2}}) \subseteq \mathbb{Q}(\zeta_{16})$ and $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ is a $\mathbb{Q}^*\langle \zeta_{16} \rangle$ -Kneser extension. In this subsection we introduce strongly G -Kneser extensions. These extensions are G -Kneser extensions E/F such that every subextension K/F of E/F is $K^* \cap G$ -Kneser. It turns out that such extensions are precisely the G -Kneser extensions with G/F^* -Cogalois correspondence.

In the remaining part of this section E/F will denote a fixed G -radical extension. Recall that

$$\mathcal{G} := \{H \mid F^* \leq H \leq G\},$$

$$\xi := \underline{\text{Intermediate}}(E/F) = \{K \mid F \subseteq K, K \text{ subfield of } E\}.$$

Proposition 3.5.7. *Let E/F be a finite G -Kneser extension, and let K be an intermediate field of E/F . Then, the following assertions are equivalent.*

- (1) K/F is H -Kneser for some $H \in \mathcal{G}$.
- (2) K/F is $K^* \cap G$ -Kneser.
- (3) E/K is K^*G -Kneser.

Proof. (2) \implies (1) is obvious.

(1) \implies (3) : Let K/F be a H -Kneser extension, for some $H \in \mathcal{G}$. Then, $K = F(H)$ and $[K : F] = |H/F^*|$. By Proposition 3.3.10, $F(H) \cap G = K \cap G = K^* \cap G = H$. We have also $E = F(G)$, but $F \subseteq K$ and so, $E = F(G) \subseteq K(G)$. So, we obtain $E = K(G) = K(K^*G)$. But we know that

$$(K^*G)/K^* \cong G/(K^* \cap G) = G/H.$$

Since G/F^* is finite and $F^* \leq H \leq G$, clearly, G/H is finite. So, this implies that $(K^*G)/K^*$ is finite. Since $F^* \leq G \leq T(E/F)$, we have

$$K^* \leq K^*F^* \leq K^*G \leq K^*T(E/F).$$

Clearly, we can see that $K^* \leq K^*G \leq T(E/K)$. Hence, E/K is a K^*G -radical extension. We also have

$$[E : K] = [E : F]/[K : F] = |G/F^*|/|H/F^*| = |G/H| = |(K^*G)/K^*|,$$

thus, E/K is a K^*G -Kneser extension.

(3) \implies (2) : Now suppose that E/K is K^*G -Kneser. Then,

$$[E : K] = |(K^*G)/K^*| = |G/(K^* \cap G)|.$$

So, $[K : F] = [E : F]/[E : K] = |G/F^*|/|G/(K^* \cap G)| = |(K^* \cap G)/F^*|$. By Proposition 3.3.10 again we have, $F(K^* \cap G)/F$ is $K^* \cap G$ -Kneser. So,

$$[F(K^* \cap G) : F] = |(K^* \cap G)/F^*| = [K : F].$$

But $F(K^* \cap G) \subseteq F(K^*) \subseteq K(K^*) = K$. Thus, we obtain $K = F(K^* \cap G)$. Therefore, K/F is $K^* \cap G$ -Kneser. \square

Proposition 3.5.8. *Let $F \subseteq K \subseteq E$ be a tower of fields, and let G be a group such that $F^* \leq G \leq E^*$. If K/F is $K^* \cap G$ -Kneser and E/K is K^*G -Kneser, then E/F is G -Kneser.*

Proof. First we have to show that E/F is G -radical. By hypothesis $K = F(K^* \cap G)$, and $E = K(K^*G)$. So, $K \subseteq F(G)$ hence $E \subseteq F(G)$. Thus, we have $E = F(G)$. Since E/K is K^*G -radical, $(K^*G)/K^*$ is a torsion group. So, for $g \in G \subseteq K^*G$ there exists some $m \in \mathbb{N}^*$ such that $g^m \in K^*$. Also, we have that K/F is $K^* \cap G$ -radical. Then, $(K^* \cap G)/F^*$ is a torsion group. Since $g^m \in K^* \cap G$, there exists some $n \in \mathbb{N}^*$ such that $g^{mn} = (g^m)^n \in F^*$. So we can deduce that G/F^* is a torsion group. Hence, E/F is a G -radical extension. On the other hand we have

$$\begin{aligned} [E : F] &= [E : K] \cdot [K : F] = |(K^*G)/K^*| \cdot |(K^* \cap G)/F^*| \\ &= |G/(K^* \cap G)| \cdot |(K^* \cap G)/F^*| = |G/F^*|. \end{aligned}$$

Therefore, E/F is a G -Kneser extension. \square

Now we can bring Propositions 3.5.7 and 3.5.8 together in the following theorem.

Theorem 3.5.9. *Let $F \subseteq K \subseteq E$ be a tower of fields, and let G be a group such that $F^* \leq G \leq E^*$. Consider the following assertions:*

- (1) K/F is $K^* \cap G$ -Kneser.
- (2) E/K is K^*G -Kneser.
- (3) E/F is G -Kneser.

Then any two of the assertions (1) – (3) imply the remaining one.

Example 3.5.10. By $\sqrt[4]{-9}$, we denote one of the complex roots, say $\sqrt{6}(1+i)/2$, of the irreducible polynomial $f = X^4 + 9 \in \mathbb{Q}[X]$. Applying Eisenstein Criterion to the polynomial $f(X+1)$, we can deduce that $f(X+1)$ is irreducible over \mathbb{Q} , hence f is irreducible over \mathbb{Q} . Now we have

$$\mathbb{Q}^* \langle \sqrt[4]{-9} \rangle / \mathbb{Q}^* = \left\{ \widehat{1}, \widehat{\sqrt[4]{-9}}, \widehat{(\sqrt[4]{-9})^2}, \widehat{(\sqrt[4]{-9})^3} \right\}.$$

So,

$$|\mathbb{Q}^*\langle\sqrt[4]{-9}\rangle/\mathbb{Q}^*| = 4 = [\mathbb{Q}(\sqrt[4]{-9}) : \mathbb{Q}].$$

Hence, $\mathbb{Q}(\sqrt[4]{-9})/\mathbb{Q}$ is a $\mathbb{Q}^*\langle\sqrt[4]{-9}\rangle$ -Kneser extension. We have

$$(\sqrt[4]{-9})^2 = (\sqrt{6}(1+i)/2)^2 = 6/4(2i) = 3i.$$

So, $i = (\sqrt[4]{-9})^2/3 \in \mathbb{Q}(\sqrt[4]{-9})$. Hence,

$$\sqrt{6} = (2\sqrt[4]{-9})/(1+i) \in \mathbb{Q}(\sqrt[4]{-9}).$$

Then we have $\mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt[4]{-9})$. So, it is natural to consider the intermediate field $K = \mathbb{Q}(\sqrt{6})$ of the extension $\mathbb{Q}(\sqrt[4]{-9})/\mathbb{Q}$. Now we claim that $\mathbb{Q}(\sqrt[4]{-9})/K$ is not a $K^*\mathbb{Q}^*\langle\sqrt[4]{-9}\rangle$ -Kneser extension. If it were then we have

$$\begin{aligned} 2 &= [\mathbb{Q}(\sqrt[4]{-9}) : K] = [\mathbb{Q}(\sqrt[4]{-9}) : \mathbb{Q}(\sqrt{6})] \\ &= |(K^*\mathbb{Q}^*\langle\sqrt[4]{-9}\rangle)/K^*| = |\mathbb{Q}^*\langle\sqrt[4]{-9}\rangle/(\mathbb{Q}(\sqrt{6})^* \cap \mathbb{Q}^*\langle\sqrt[4]{-9}\rangle)| = |\mathbb{Q}^*\langle\sqrt[4]{-9}\rangle/\mathbb{Q}^*| = 4. \end{aligned}$$

But this is a contradiction. So, by Proposition 3.5.7, $\mathbb{Q}(\sqrt[4]{-9})/\mathbb{Q}$ is not a H -Kneser extension for every H with $\mathbb{Q}^* \leq H \leq \mathbb{Q}^*\langle\sqrt[4]{-9}\rangle$. On the other hand $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$ is $\mathbb{Q}^*\langle\sqrt{6}\rangle$ -Kneser extension. \square

Now we have the following definition.

Definition 3.5.11. *A finite extension E/F is said to be strongly G -Kneser if it is a G -radical extension such that the extension E/K is K^*G -Kneser for every intermediate field K of E/F .*

The extension E/F is called strongly Kneser if it is strongly G -Kneser for some group G .

So, the extension in Example 4.4.10 is not a strongly G -Kneser extension.

The following theorem reformulates the concept of strongly G -Kneser extension.

Theorem 3.5.12. *The following statements are equivalent for a finite G -radical extension E/F .*

- (1) E/F is strongly G -Kneser.
- (2) K/F is $K^* \cap G$ -Kneser for every intermediate field K of E/F .
- (3) E/K is K^*G -Kneser for every intermediate field K of E/F .
- (4) $[E : K] = |G/(K^* \cap G)|$ for every intermediate field K of E/F .
- (5) $[K : F] = |(K^* \cap G)/F^*|$ for every intermediate field K of E/F .

Proof. The equivalences (1) \iff (2) \iff (3) follows from Proposition 3.5.7. The implications (2) \implies (5) and (3) \implies (4) are clear.

(5) \implies (2) : In (5) we can take as K the field E , so we obtain

$$[E : F] = |(E^* \cap G)/F^*| = |G/F^*|.$$

But we also know that E/F is a G -radical extension, so E/F is a G -Kneser extension.

Let K an arbitrary intermediate field of the extension E/F . Then, by Proposition 3.3.10, $F(K^* \cap G)/F$ is $K^* \cap G$ -Kneser. So, $[F(K^* \cap G) : F] = |(K^* \cap G)/F^*|$. But by hypothesis we have $[K : F] = |(K^* \cap G)/F^*|$. So, $[F(K^* \cap G) : F] = [K : F]$. Clearly, $F(K^* \cap G) \subseteq F(K^*) \subseteq K(K^*) = K$. Thus, $K = F(K^* \cap G)$. Therefore, K/F is a $K^* \cap G$ -Kneser extension.

(4) \implies (5) : In (4) we can take as K the field F and we obtain

$$[E : F] = |G/(F^* \cap G)| = |G/F^*|.$$

Since E/F is also a G -radical extension, we have that E/F is a G -Kneser extension.

For any intermediate field K of E/F , we have

$$[K : F] = [E : F]/[E : K] = |G/F^*|/|G/(K^* \cap G)| = |(K^* \cap G)/F^*|,$$

as desired. □

In the proof of the above theorem, we can easily see that any strongly G -Kneser extension is G -Kneser, but the converse does not hold in general, as we can see in Example 3.5.10.

The following result provides a characterization of G -Kneser extensions E/F for which the standard Cogalois connection becomes a bijective correspondence between

ξ and \mathcal{G} , where

$$\mathcal{G} := \{H \mid F^* \leq H \leq G\},$$

$$\xi := \underline{\text{Intermediate}}(E/F) = \{K \mid F \subseteq K, K \text{ subfield of } E\}.$$

This result will be the dual version of the corresponding result for Galois extensions which we stated in the Proposition 3.5.4.

Theorem 3.5.13. *The following assertions are equivalent for a finite G -radical extension E/F .*

- (1) E/F is strongly G -Kneser.
- (2) E/F is G -Kneser, and the map $\psi : \mathcal{G} \rightarrow \xi$, $\psi(H) = F(H)$, is surjective.
- (3) E/F is G -Kneser, and every element of ξ is a closed element in the standard Cogalois connection associated with E/F .
- (4) E/F is G -Kneser, and the map $\varphi : \xi \rightarrow \mathcal{G}$, $\varphi(K) = K \cap G$, is injective.
- (5) E/F is G -Kneser, and the maps $- \cap G : \xi \rightarrow \mathcal{G}$, $F(-) : \mathcal{G} \rightarrow \xi$ are isomorphisms of lattices, inverse to one another.
- (6) E/F is a G -Kneser extension with G/F^* -Cogalois correspondence.

Proof. (1) \implies (2) : Suppose that E/F is a strongly G -Kneser extension, and let K be in ξ . By Theorem 3.5.12, the extension K/F is $K^* \cap G$ -Kneser. So, we have $K = F(K^* \cap G)$. Now let $H = K \cap G = K^* \cap G \in \mathcal{G}$. So, $K = F(H) = \psi(H)$. Hence, ψ is surjective.

(2) \iff (3) follows from Proposition 3.5.3 (2).

(2) \implies (4) : Let $K_1, K_2 \in \xi$ be such that $\varphi(K_1) = \varphi(K_2)$. So, $K_1 \cap G = K_2 \cap G$. By hypothesis ψ is surjective. Then, there exists $H_1, H_2 \in \mathcal{G}$ such that $K_1 = F(H_1)$ and $K_2 = F(H_2)$. So, we obtain $K_1 \cap G = F(H_1) \cap G$ and $K_2 \cap G = F(H_2) \cap G$. But by Proposition 3.3.10, we have $F(H_1) \cap G = H_1$ and $F(H_2) \cap G = H_2$. Thus, $K_1 \cap G = H_1$ and $K_2 \cap G = H_2$. But we assumed at the beginning of this paragraph that $K_1 \cap G = K_2 \cap G$. Hence, $H_1 = H_2$. Therefore, $K_1 = K_2$, and so φ is injective.

(4) \implies (5) : For all $H \in \mathcal{G}$, we have

$$(\varphi \circ \psi)(H) = \varphi(\psi(H)) = \varphi(F(H)) = F(H) \cap G = H,$$

by Proposition 3.3.10. So, $\varphi \circ \psi = 1_{\mathcal{G}}$. This shows that φ is surjective. By hypothesis we know that φ is injective, hence φ is bijective and ψ is its inverse. Thus, φ and ψ are isomorphisms of posets, and also isomorphisms of lattices inverse to one another.

(5) \implies (1) : Let $K \in \xi$. Using Theorem 3.5.12, it is enough to show that K/F is $K^* \cap G$ -Kneser. By hypothesis, ψ is surjective. So, there exists $H \in \mathcal{G}$ such that $K = \psi(H) = F(H)$. But the maps ψ and φ are inverse to one another, so we have $H = \varphi(K) = K \cap G = K^* \cap G$. By Proposition 3.3.10, $F(H)/F$ is H -Kneser, in other words, K/F is $K^* \cap G$ -Kneser.

(5) \iff (6) : Now we denote $\tilde{\mathcal{G}}$ the lattice Subgroups (G/F^*) of all subgroups of the quotient group $\tilde{G} = G/F^*$. Clearly, the lattices \mathcal{G} and $\tilde{\mathcal{G}}$ are canonically isomorphic. So, the Cogalois connection associated with E/F

$$\xi \begin{array}{c} \xrightarrow{\varphi} \\ \xleftarrow{\psi} \end{array} \mathcal{G}$$

can be expressed equivalently using the Cogalois connection

$$\xi \begin{array}{c} \xrightarrow{\varphi} \\ \xleftarrow{\psi} \end{array} \tilde{\mathcal{G}},$$

where $\tilde{\varphi}(K) = (K \cap G)/F^*$ and $\tilde{\psi}(H/F^*) = F(H)$. Thus, the maps $- \cap G : \xi \longrightarrow \mathcal{G}$, and $F(-) : \mathcal{G} \longrightarrow \xi$ are isomorphisms of lattices, inverse to one another if and only if the maps

$$\tilde{\varphi} : \xi \longrightarrow \tilde{\mathcal{G}}$$

and

$$\tilde{\psi} : \tilde{\mathcal{G}} \longrightarrow \xi$$

are lattice isomorphisms, inverse to one another. So, by Definition 3.5.5, if and only if E/F is an extension with G/F^* -Cogalois correspondence. \square

In the next result we see that the quotient extensions and subextensions of strongly Kneser extensions are also strongly Kneser.

Proposition 3.5.14. *Let E/F be a strongly G -Kneser extension. Then for any intermediate field K , the following assertions hold.*

(1) K/F is strongly $K^* \cap G$ -Kneser.

(2) E/K is strongly K^*G -Kneser.

Proof. (1) Let L be an intermediate field of the extension K/F . Then by Theorem 3.5.13, there exists $H \in \mathcal{G}$ with $L = F(H)$. We have $F^* \leq H \leq G$. Clearly we have, $H \leq F(H)^* = L^* \leq K^*$ and $H \leq G$. So, $F^* \leq H \leq K^* \cap G$. Since $L = F(H)$, by Theorem 3.5.13 again, we have K/F is strongly $K^* \cap G$ -Kneser.

(2) Let M be a subfield of E with $K \subseteq M \subseteq E$. Since E/F is strongly G -Kneser, by Theorem 3.5.12, E/M is M^*G -Kneser. Clearly, $M^*G = M^*(K^*G)$ since $K^* \subseteq M^*$. So, E/M is $M^*(K^*G)$ -Kneser. Since M is arbitrary, by Theorem 3.5.12 again, E/K is strongly K^*G -Kneser. \square

3.5.3 G -Cogalois Extensions

In this section we investigate G -Cogalois extensions. G -Cogalois extensions in Cogalois Theory plays the same role as that of Galois extensions in Galois Theory. A G -Cogalois extension is defined as a separable G -Kneser extension with G/F^* -Cogalois correspondence.

Using the concept of “local purity” which we called as n -purity, where n is the exponent of the finite group G/F^* , we can characterize G -Cogalois extensions E/F in the class of G -Kneser extensions.

Now we recall Definition 3.4.1 which says that the extension E/F is called *pure* when $\mu_p(E) \subseteq F$, for all $p \in \mathcal{P}$.

The next definition defines the concept of “local purity”.

Definition 3.5.15. Let E/F be an arbitrary extension and let $n \in \mathbb{N}^*$. The extension E/F is called n -pure if $\mu_p(E) \subseteq F$, for every $p \in \mathcal{P}_n$. \square

It can easily be seen that an extension E/F is pure if and only if it is n -pure for every $n \in \mathbb{N}^*$. It is clear that an n -pure extension is not necessarily pure. Consider the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. This extension is 2-pure, since $\mathcal{P}_2 = \mathcal{P} \cap \mathbb{D}_2 = \emptyset$. But

this extension is not 3-pure. Since $\mathcal{P}_3 = \{3\}$, and for $p = 3 \in \mathcal{P}_3$, we have that $\mu_3(\mathbb{Q}(\sqrt{-3})) = \{1, (-1 \pm \sqrt{-3})/2\} \not\subseteq \mathbb{Q}$. So the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is not pure.

The next result which characterizes the strongly Kneser extensions in terms of standard Cogalois connection is more stronger than Theorem 3.5.13. This time the extension E/F is separable.

Theorem 3.5.16. (*The n -Purity Criterion*) *The following assertions are equivalent for a finite separable G -radical extension E/F with G/F^* finite and $n = \exp(G/F^*)$.*

- (1) E/F is strongly G -Kneser.
- (2) E/F is G -Kneser, and the map $\psi : \mathcal{G} \rightarrow \xi$, $\psi(H) = F(H)$, is surjective.
- (3) E/F is G -Kneser, and every element of ξ is a closed element in the standard Cogalois connection associated with E/F .
- (4) E/F is G -Kneser, and the map $\varphi : \xi \rightarrow \mathcal{G}$, $\varphi(K) = K \cap G$, is injective.
- (5) E/F is G -Kneser, and the maps $- \cap G : \xi \rightarrow \mathcal{G}$, $F(-) : \mathcal{G} \rightarrow \xi$ are isomorphisms of lattices, inverse to one another.
- (6) E/F is a G -Kneser extension with G/F^* -Cogalois correspondence.
- (7) E/F is n -pure.

Proof. In the proof of Theorem 3.5.13 we have shown that the equivalences (1) through (6) hold for extensions which are necessarily separable.

(7) \implies (1) : Suppose that the extension E/F is n -pure. Let $K \in \xi$ be arbitrary. We are going to use Theorem 3.5.12, so it is enough to show that K/F is $K^* \cap G$ -Kneser. For this we can use Kneser Criterion (Theorem 3.3.12). Let p be an odd prime such that $\zeta_p \in K^* \cap G$. Our aim is to show that $\zeta_p \in F$. If $p|n$, then $p \in \mathcal{P} \cap \mathbb{D}_n = \mathcal{P}_n$. So $\mu_p(E) \subseteq F$, by n -purity; hence, $\zeta_p \in F$. If $\gcd(p, n) = 1$, then there exists some $a, b \in \mathbb{Z}$ such that $ap + bn = 1$. Hence,

$$\zeta_p = \zeta_p^{ap+bn} = \zeta_p^{bn} \in F^*,$$

since $n = \exp(G/F^*)$ implies that $G^n \subseteq F^*$ by Definition 3.2.3.

Now suppose that $1 + \zeta_4 \in K^* \cap G$. Then we should have $\text{Char}(F) \neq 2$. For otherwise $(1 + \zeta_4)^4 = 1 + \zeta_4^4 = 0 \in K^* \cap G$, which is a contradiction.

Let $m = \text{ord}(\widehat{1 + \zeta_4})$. By previous results $(1 + \zeta_4)^4 = -4 \in F^*$, so $m \in \{1, 2, 4\}$. If $m = 1$, then $1 + \zeta_4 \in F^*$. If $m = 2$, then $(1 + \zeta_4)^2 = 2\zeta_4 \in F^*$. Since, $\text{Char}(F) \neq 2$, $\zeta_4 \in F^*$. If $m = 4$, then clearly $4 \mid n$, since $G^m \subseteq F^*$. But $1 + \zeta_4 \in K^* \cap G \subseteq E$. So, $\zeta_4 \in E$, and by n -purity this implies that $\zeta_4 \in F$. Thus, K/F is $K^* \cap G$ -Kneser, and so, E/F is strongly G -Kneser.

(2) \implies (7) : Now suppose that the extension E/F is G -Kneser and the map ψ is surjective. Our aim is to show that for all $p \in \mathcal{P}_n$, $\mu_p(E) \subseteq F$. Then we deduce that E/F is pure. Now let p be an odd prime with $p \mid n$. Then by Proposition 3.2.5 there exists $g \in G$ such that $\text{ord}(\widehat{g}) = p$. By Proposition 3.3.10, the extension $F(F^*\langle g \rangle)/F$ is $F^*\langle g \rangle$ -Kneser. So,

$$[F(g) : F] = [F(F^*\langle g \rangle) : F] = |F^*\langle g \rangle/F^*| = |\langle g \rangle| = p. \quad (3.5.1)$$

Assume that $\zeta_p \in E$. Clearly, $X^p - g^p \in F[X]$, since $\text{ord}(\widehat{g}) = p$ implies that $g^p \in F^*$. Also g is a root of this polynomial, and by Equation (3.5.1) we have, $\text{Min}(g, F) = X^p - g^p$. Then we have $\text{Min}(\zeta_p g, F) = X^p - g^p$, so $[F(\zeta_p g) : F] = p$. Since $F(\zeta_p g) \in \xi$, and ψ is surjective, there exists $h \in G$ such that

$$F(\zeta_p g) = F(h) = F(F^*\langle h \rangle),$$

where $\text{ord}(\widehat{h}) = p$, since $[F(h) : F] = p$. So we obtain $\zeta_p g \in F(h)$. Then, $\zeta_p \in F(h, g)$. The subgroups $\langle \widehat{g} \rangle, \langle \widehat{h} \rangle$ of G/F^* have the same order, so they are either equal or they have empty intersection. If they have empty intersection, then $\langle \widehat{g}, \widehat{h} \rangle = \langle \widehat{g} \rangle \oplus \langle \widehat{h} \rangle$. By Proposition 3.3.10, we know that the extension $F(F^*\langle g, h \rangle)/F$ is $F^*\langle g, h \rangle$ -Kneser. Thus,

$$[F(g, h) : F] = [F(F^*\langle g, h \rangle) : F] = |F(F^*\langle g, h \rangle)/F^*| = |\langle \widehat{g}, \widehat{h} \rangle| \in \{p, p^2\}.$$

We know that $F \subseteq F(\zeta_p) \subseteq F(g, h)$, and $[F(\zeta_p) : F] \leq p - 1$, so $[F(\zeta_p) : F] = 1$, since $[F(g, h) : F] \in \{p, p^2\}$ and $[F(\zeta_p) : F]$ must divide $[F(g, h) : F]$. Hence, $\zeta_p \in F$, as desired.

Suppose that $4 \mid n$ and $\zeta_4 \in E \setminus F$. Now try to get a contradiction. We should have $\text{Char}(F) \neq 2$. By Proposition 3.2.5 again, G/F^* contains an element of order 4, say

\widehat{g} . Since $F(\zeta_4) \in \xi$, and ψ is surjective, there exists $h \in G$ such that

$$F(\zeta_4) = F(h) = F(F^*\langle h \rangle).$$

We have that $\text{ord}(h) = 2$, since $[F(\zeta_4) : F] = 2$. Hence, $\zeta_4 \in F(h)$, which implies that $\zeta_4 = \lambda + \mu h$, for some $\lambda, \mu \in F$. Then, $(\zeta_4)^2 = -1 = \lambda^2 + 2\lambda\mu h + \mu^2 h^2$. But $h^2 \in F$, since $\text{ord}(h) = 2$. So we should have that $2\lambda\mu = 0$. By hypothesis, $\zeta_4 \notin F$, so $\mu \neq 0$. Then we should have that $\lambda = 0$. Hence, $\zeta_4 = \mu h$, and so $\zeta_4 \in G$. Now put $K = F((1 + \zeta_4)g)$. Then, we use the implication (2) \implies (1) and Theorem 3.5.12 to obtain E/K is K^*G -Kneser. Since $1 + \zeta_4 = (1 + \zeta_4)gg^{-1} \in K^*G$, by Kneser Criterion we have $\zeta_4 \in K$. We know that $[(1 + \zeta_4)g]^4 = -4g^4 \in F^*$, since $\text{ord}(\widehat{g}) = 4$. So this clearly implies that $[K : F] \leq 4$. Since $\zeta_4 \in K$, and $[K : F] \leq 4$, we have that

$$\begin{aligned} \zeta_4 &= \lambda_0 + \lambda_1(1 + \zeta_4)g + \lambda_2(1 + \zeta_4)^2g^2 + \lambda_3(1 + \zeta_4)^3g^3 \\ &= \lambda_0 + \lambda_1g + \lambda_1\zeta_4g + 2\lambda_2\zeta_4g^2 + 2\lambda_3\zeta_4g^3 - 2\lambda_3g^3, \end{aligned}$$

for some $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in F$. Since $\{1, \zeta_4, g, \zeta_4g, \zeta_4g^2, \zeta_4g^3, g^3\} \subseteq G$ is linearly dependent over F , by Corollary 3.3.9 we should have that ζ_4 must be congruent modulo F^* with one of the following elements

$$1, g, \zeta_4g, \zeta_4g^2, \zeta_4g^3, g^3.$$

But $\text{ord}(\widehat{\zeta}) = 2$, and $\text{ord}(\widehat{g}) = 4$, so the only possibility we can have is that $\widehat{\zeta}_4 = \widehat{1}$. Thus, $\zeta_4 \in F^*$, which contradicts our hypothesis, since we assumed that $\zeta_4 \notin F$. Hence we are done. \square

In the class of finite extensions E/F with G/F^* Cogalois correspondence the most important ones are those which have the property of being separable also. In the following definition we give them a special name.

Definition 3.5.17. *An extension E/F is called G -Cogalois if it is a separable strongly G -Kneser extension.* \square

Remark 3.5.18. A strongly G -Kneser extension is not necessarily separable, as the example in Remark 3.4.9 shows. \square

The next result shows that the subextensions and quotient extensions of a G -Cogalois extension are also G -Cogalois.

Proposition 3.5.19. *Let E/F be a G -Cogalois extension. Then for any intermediate field K of E/F , the following assertions hold.*

- (1) K/F is $K^* \cap G$ -Cogalois.
- (2) E/K is K^*G -Cogalois.

Proof. By Proposition 3.5.14, the result follows immediately. \square

3.5.4 The Kneser group of a G -Cogalois extension

In this section we are going to show that a separable G -Kneser extension is G -Cogalois if and only if the group G has a prescribed structure. Then, consequently we can say that the group G/F^* of any G -Cogalois extension E/F is uniquely determined. This group is called the *Kneser group* of E/F and denoted by $\text{Kne}(E/F)$.

If A is a multiplicative group with identity element e , then for any $p \in \mathbb{P}$ we denote by

$$t_p(A) = \{x \in A \mid x^{p^n} = e \text{ for some } n \in \mathbb{N}\}$$

the p *primary component* of the group A . Now recall that we have denoted by $\text{Cog}(E/F)$, the torsion subgroup of the quotient group E^*/F^* . By $\text{Cog}_2(E/F)$, we are going to denote the subgroup of $\text{Cog}(E/F)$ consisting of all its elements of order ≤ 2 .

Theorem 3.5.20. *Let E/F be a separable G -Kneser extension with $n = \exp(G/F^*)$.*

- (1) *Suppose that $4 \nmid n - 2$. Then E/F is a G -Cogalois extension if and only if*

$$G/F^* = \bigoplus_{p \in \mathbb{P}_n} t_p(\text{Cog}(E/F)).$$

(2) Suppose that $n \equiv 2 \pmod{4}$. Then E/F is a G -Cogalois extension if and only if

$$G/F^* = \left(\bigoplus_{p \in \mathbb{P}_n \setminus \{2\}} t_p(\text{Cog}(E/F)) \right) \bigoplus \text{Cog}_2(E/F).$$

□

Corollary 3.5.21. Let E/F be an extension which is simultaneously G -Cogalois and H -Cogalois. Then $G = H$.

Proof. Let $m = \exp(G/F^*)$, $n = \exp(H/F^*)$, and $k = [E : F]$. Then we have

$$|G/F^*| = |H/F^*| = [E : F] = k.$$

By Proposition 3.2.7, the order and exponent of a finite Abelian group have the same prime divisors. So we have $\mathbb{P}_n = \mathbb{P}_m = \mathbb{P}_k$. Using Theorem 3.5.20, it is enough prove that $4 \mid n$ if and only if $4 \mid m$.

Suppose that $4 \mid m$. Then by Proposition 3.2.5, G/F^* contains an element of order 4, say \hat{g} . Now set $G_1 = F^*\langle \hat{g} \rangle$ and $E_1 = F(G_1)$. By Theorem 3.5.16 (2), there exists H_1 such that $F^* \leq H_1 \leq H$, $E_1 = F(H_1)$. Clearly, $|H_1/F^*| = 4$. By Proposition 3.5.19, E_1/F is $E_1^* \cap G$ -Cogalois. We have $E_1^* \cap G = E_1 \cap G = F(G_1) \cap G = G_1$ by Proposition 3.3.10. Hence, E_1/F is a G_1 -Cogalois extension. Similarly, we can also show that E_1/F is a H_1 -Cogalois extension. By Theorem 3.5.16, we know that there is a bijective Cogalois correspondence between the lattice of all intermediate fields of the extension E_1/F and the lattice of all subgroups of the cyclic group G_1/F^* of order 4. So, E_1/F has only one proper intermediate field. Now we can use the bijective Cogalois correspondence between the lattice of all intermediate fields of the extension E_1/F and the lattice of all subgroups of H_1/F^* , and deduce that the quotient group H_1/F^* of order 4 has only one proper subgroup. Hence, this group is necessarily cyclic and clearly, $4 \mid n$. The other inclusion can be shown in a similar way. Hence, we are done. □

So, for any G -Cogalois extension, the uniqueness of the group G is deduced. Now the following concept make sense.

Definition 3.5.22. *If E/F is a G -Cogalois extension, then the group G/F^* is called the Kneser group of the extension E/F and is denoted by $\text{Kne}(E/F)$. \square*

3.5.5 Galois G -Cogalois Extensions

In this section we are going to deal with finite field extensions which are simultaneously Galois and G -Cogalois. Firstly, we characterize G -radical extensions, not necessarily finite, which are separable or Galois.

Galois G -radical Extensions

Recall that for any torsion group T with identity element e , we introduced in Section 3.2 the notation:

$$\mathcal{O}_T = \{\text{ord}(x) \mid x \in T\}.$$

When the subset \mathcal{O}_T of \mathbb{N} is a bounded set, or a finite set, then we say that the torsion group T is a *group of bounded order*, and the least number $n \in \mathbb{N}^*$ with the property that $T^n = \{e\}$ is the *exponent* $\text{exp}(T)$ of T . The group T is *n -bounded* if T is a group of bounded order and $\text{exp}(T) = n$.

We know that for any G -radical extension E/F , which is not necessarily finite, the group G/F^* is a torsion Abelian group. So, we can consider the subset of natural numbers, \mathcal{O}_{G/F^*} .

Definition 3.5.23. *A G -radical extension E/F , which is not necessarily finite, is said to be a bounded extension if G/F^* is a group of bounded order; in this case, if $\text{exp}(G/F^*) = n$, we say that E/F is an n -bounded extension. \square*

If E/F is an n -bounded extension, then Remark 3.2.6 implies that

$$\mathcal{O}_{G/F^*} = \mathbb{D}_n.$$

Now we list some important results which will be needed in the remaining part of the Thesis.

Lemma 3.5.24. *Let E/F be a G -radical extension which is not necessarily finite. Then E/F is separable if and only if $\gcd(m, e(F)) = 1$ for all $m \in \mathcal{O}_{G/F^*}$. \square*

Corollary 3.5.25. *Let E/F be an n -bounded G -radical extension, which is not necessarily finite. Then E/F is a separable extension if and only if $\gcd(n, e(F)) = 1$. \square*

Corollary 3.5.26. *Let E/F be a finite G -radical extension with G/F^* finite, and let $n = \exp(G/F^*)$. Then E/F is separable if and only if $\gcd(n, e(F)) = 1$. \square*

Proposition 3.5.27. *Let E/F be a G -radical extension, which is not necessarily finite. Then E/F is a Galois extension if and only if $\gcd(m, e(F)) = 1$ and $\zeta_m \in E$ for all $m \in \mathcal{O}_{G/F^*}$. \square*

Corollary 3.5.28. *Let E/F be an n -bounded G -radical extension. Then E/F is a Galois extension if and only if $\gcd(n, e(F)) = 1$ and $\zeta_n \in E$. \square*

Corollary 3.5.29. *Let E/F be a finite G -radical extension with G/F^* a finite group of exponent n . Then E/F is a Galois extension if and only if $\gcd(n, e(F)) = 1$ and $\zeta_n \in E$. \square*

Abelian G -Cogalois Extensions

In this subsection we provide an important result which says that the Kneser group and the Galois group of any finite Abelian G -Cogalois extension are isomorphic.

Theorem 3.5.30. *For any finite Abelian G -Cogalois extension E/F , the groups $\text{Gal}(E/F)$ and $\text{Kne}(E/F)$ are isomorphic. \square*

Corollary 3.5.31. *For any finite Abelian Cogalois extension E/F , the groups $\text{Gal}(E/F)$ and $\text{Cog}(E/F)$ are isomorphic. \square*

Proof. The extension E/F is clearly a $T(E/F)$ -Kneser extension. So, by Theorem 3.5.32 in the following section, E/F is $T(E/F)$ -Cogalois. Hence, $\text{Gal}(E/F)$ is isomorphic to $\text{Kne}(E/F) = T(E/F)/F^* = \text{Cog}(E/F)$ by Theorem 3.5.30. \square

3.5.6 Some Examples of G -Cogalois Extensions

In this section we are going to present some examples of G -Cogalois extensions. Firstly, we give a result which helps us to determine some G -Cogalois extensions.

Theorem 3.5.32. *Any finite Cogalois extension E/F is $T(E/F)$ -Cogalois.*

Proof. By the Greither-Harrison Criterion (Theorem 3.4.6), the extension E/F is separable and pure. So, it is n -pure for all $n \in \mathbb{N}^*$. In particular we have that E/F is $n = \exp(T(E/F)/F^*)$ -pure. So, E/F is strongly $T(E/F)$ -Kneser by Theorem 3.5.16. But E/F is also separable, hence the extension E/F is $T(E/F)$ -Cogalois. \square

Examples 3.5.33. (1) In Proposition 3.4.13, we have shown that the extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ are Cogalois. Also we have shown that

$$[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}(\sqrt{2})] = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

So, the extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ are finite. Now we can use Theorem 3.5.32 and obtain $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is $\mathbb{Q}^*\langle\sqrt{2}\rangle$ -Cogalois and $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ is $\mathbb{Q}^*\langle\sqrt{1+\sqrt{2}}\rangle$ -Cogalois.

(2) By Corollary 3.4.16, we know that the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is Cogalois if and only if $d \neq -1, -3$ where $d \neq 1$ is a square-free rational integer. Again we can use Theorem 3.5.32 to deduce that the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is $\mathbb{Q}^*\langle\sqrt{d}\rangle$ -Cogalois, where $d \neq -1, -3$.

In Remark 3.3.11 we have shown that the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -Kneser. So, it is $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -radical. But this extension is also separable and finite. We also have $\mathbb{Q}^*\langle\sqrt{-3}\rangle/\mathbb{Q}^* = \{\widehat{1}, \widehat{\sqrt{-3}}\}$. So, $\exp(\mathbb{Q}^*\langle\sqrt{-3}\rangle/\mathbb{Q}^*) = 2$. But it is clear that this extension is 2-pure. Hence by Theorem 3.5.16, $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is strongly $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -Kneser. Thus, it is $\mathbb{Q}^*\langle\sqrt{-3}\rangle$ -Cogalois. Similarly we can show that the extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ is $\mathbb{Q}^*\langle\sqrt{-1}\rangle$ -Cogalois. So, we deduce that any quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where $d \neq 1$ is a square-free rational integer, is $\mathbb{Q}^*\langle\sqrt{d}\rangle$ -Cogalois.

Also we know that any quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, where $d \neq 1$ is a square-free rational integer is a Galois extension, since $\mathbb{Q}(\sqrt{d})$ is a splitting field of some

separable polynomial. Galois group of this extension has order 2, so it is cyclic. Hence, $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is an Abelian G -Cogalois extension. Thus by Corollary 3.5.31, $\text{Kne}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ and $\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ are isomorphic, where $d \neq 1$ is a square-free rational integer.

(3) By Examples 3.4.10, we know that the extension

$$\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q},$$

with $r \in \mathbb{N}^*$, $a_1, \dots, a_r, n_1, \dots, n_r \in \mathbb{N}^*$ and $\sqrt[n_i]{a_i}$ is a positive real n_i -th root of a_i , for all i , $1 \leq i \leq r$ is a finite Cogalois extension. So, again by Theorem 3.5.32, this extension is $T(\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q})$ -Cogalois. But again by Examples 3.4.10, we have

$$T(\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q}) = \mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle.$$

So, this extension is $\mathbb{Q}^* \langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle$ -Cogalois.

(4) Suppose that α can be written as a finite sum of real numbers of type $\pm \sqrt[n_i]{a_i}$, $1 \leq i \leq r$ where $r, n_1, \dots, n_r, a_1, \dots, a_r \in \mathbb{N}^*$. Then the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is clearly a subextension of the extension of the extension in (3), since $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r}) \subseteq \mathbb{R}$. In (3) we have shown that $\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/\mathbb{Q}$ is Cogalois. So, by Proposition 3.4.11 we can say that the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, which is finite, is Cogalois. Again by Theorem 3.5.32, we can say that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is $\mathbb{Q}^* \langle \alpha \rangle$ -Cogalois. \square

Other than finite Cogalois extensions, there are also some other large classes of G -Cogalois extensions. The n -Purity Criterion provides us with these other classes of G -Cogalois extensions: *classical finite Kummer extensions, finite generalized Kummer extensions, finite Kummer extensions with few roots of unity and finite quasi-Kummer extensions.*

Classical Kummer Extensions

Recall that Ω is a fixed algebraically closed field containing F as a subfield; and any field containing F will be a subfield of Ω . For any nonempty subset A of F^* and any

$n \in \mathbb{N}^*$, $\sqrt[n]{A}$ will denote the subset of $T(\Omega/F)$ defined by

$$\sqrt[n]{A} = \{x \in \Omega \mid x^n \in A\}.$$

In particular, if $A = \{a\}$, then $\sqrt[n]{\{a\}}$ is precisely the set of all roots in Ω of the polynomial $X^n - a \in F[X]$. $\sqrt[n]{a}$ denotes a root, which is not specified, of the polynomial $X^n - a \in F[X]$. So, $\sqrt[n]{a} \in \sqrt[n]{\{a\}}$. We have

$$\sqrt[n]{\{a\}} = \{\zeta_n^k \sqrt[n]{a} \mid 0 \leq k \leq n-1\}.$$

In particular, if $\zeta_n \in F$, then $F(\sqrt[n]{\{a\}}) = F(\sqrt[n]{a})$. If we have that F is a subfield of \mathbb{R} and $a > 0$, then $\sqrt[n]{a}$ will denote the unique positive root in \mathbb{R} of the polynomial $X^n - a$.

Definition 3.5.34. A classical n -Kummer extension, where $n \in \mathbb{N}^*$, is an Abelian extension E/F such that $\gcd(n, e(F)) = 1$, $\mu_n(F) \subseteq F$ and $\text{Gal}(E/F)$ is a group of exponent a divisor of n .

A classical Kummer extension, or just a Kummer extension is any extension which is a classical n -Kummer extension for a certain integer $n \geq 1$. If E/F is a classical Kummer extension, we also say that E is a classical Kummer extension of F . \square

Theorem 3.5.35. The following assertions are equivalent for an extension E/F and a natural number $n \geq 1$.

- (1) E/F is a classical n -Kummer extension.
- (2) $\gcd(n, e(F)) = 1$, $\mu_n(\Omega) \subseteq F$, and $E = F(\sqrt[n]{A})$ for some $\emptyset \neq A \subseteq F^*$.
- (3) $\gcd(n, e(F)) = 1$, $\mu_n(\Omega) \subseteq F$, and $E = F(B)$ for some $\emptyset \neq B \subseteq E^*$ with $B^n \subseteq F$.

\square

Corollary 3.5.36. The following assertions are equivalent for a finite extension E/F and a natural number $n \geq 1$.

- (1) E/F is a classical n -Kummer extension.
- (2) $\gcd(n, e(F)) = 1$, $\mu_n(\Omega) \subseteq F$, and $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$ for some $r \in \mathbb{N}^*$ and $\{a_1, \dots, a_r\} \in F^*$.

□

Lemma 3.5.37. Let E/F be a separable G -radical extension with G/F^* finite, and let $n \in \mathbb{N}^*$ be such that $G^n \subseteq F^*$. If the extension E/F is n -pure then E/F is G -Cogalois.

Proof. The finite group G/F^* is clearly a group of bounded order and has a finite exponent, say m . Then by Lemma 3.2.4, $m \mid n$. If we have $p \in \mathcal{P}_m$, then clearly, $p \mid n$. So by hypothesis, $\mu_p(E) \subseteq F$. But this shows that E/F is m -pure. So, by Theorem 3.5.16, E/F is G -Cogalois. □

Theorem 3.5.38. Let E/F be a finite classical n -Kummer extension where we have $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$, $n, r \in \mathbb{N}^*$ and $\{a_1, \dots, a_r\} \subseteq F^*$. Then, the following statements hold.

- (1) E/F is an $F^*\langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle$ -Cogalois extension.
- (2) The maps $H \longrightarrow F(\sqrt[n]{H})$ and $K \longrightarrow K^n \cap (F^{*n}\langle a_1, \dots, a_r \rangle)$ establish isomorphisms of lattices, inverse to one another, between the lattice of all subgroups H of $F^{*n}\langle a_1, \dots, a_r \rangle$ containing F^{*n} and the lattice of all intermediate fields K of E/F . Moreover, any subextension K/F of E/F is a classical n -Kummer extension.
- (3) If H is any subgroup of $F^{*n}\langle a_1, \dots, a_r \rangle$ containing F^{*n} , then any set of representatives of the group $\sqrt[n]{H}/F^*$ is a vector space basis of $F(\sqrt[n]{H})$ over F , and $[F(\sqrt[n]{H}) : F] = |H/F^{*n}|$. In particular, one has

$$[E : F] = |F^{*n}\langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle / F^*| = |F^{*n}\langle a_1, \dots, a_r \rangle / F^{*n}|.$$

(4) *There exists a canonical group isomorphism*

$$F^* \langle \sqrt[r]{a_1}, \dots, \sqrt[r]{a_r} \rangle / F^* \cong \text{Hom}(\text{Gal}(E/F), \mu_n(F)).$$

□

Generalized Kummer Extensions

In this subsection we investigate another class of G -Cogalois extensions. This class, namely the class of *generalized Kummer extensions* is larger than the class of classical Kummer extensions which we have presented in the previous section. This new class includes the class of *Kummer extensions with few roots of unity* that we are going to present in the following section.

The theory of finite generalized Kummer extensions can be developed using the properties of G -Cogalois extensions. These extensions in general are not Galois extensions, so Galois Theory can not be applied here as in the case of classical Kummer extensions.

Definition 3.5.39. *We say that a finite extension E/F is a generalized n -Kummer extension, where $n \in \mathbb{N}^*$, if $\gcd(n, e(F)) = 1$, $\mu_n(F) \subseteq F$, and there exists some $r \in \mathbb{N}^*$, $a_1, \dots, a_r \in F^*$ such that $E = F(\sqrt[r]{a_1}, \dots, \sqrt[r]{a_r})$.*

A generalized Kummer extension is an extension which is a generalized n -Kummer extension for some integer $n \geq 1$. □

Any classical n -Kummer extension is a generalized n -Kummer extension. By Corollary 3.5.26, any generalized Kummer extension is separable but not necessarily a Galois extension.

Lemma 3.5.40. Let E/F be a finite generalized n -Kummer extension, where we have $E = F(\sqrt[r]{a_1}, \dots, \sqrt[r]{a_r})$, $r \in \mathbb{N}^*$ and $a_1, \dots, a_r \in F^*$. Then E/F is an $F^* \langle \sqrt[r]{a_1}, \dots, \sqrt[r]{a_r} \rangle$ -Cogalois extension.

Proof. The extension E/F is G -radical, where $G = F^* \langle \sqrt[r]{a_1}, \dots, \sqrt[r]{a_r} \rangle$, and clearly $G^n \subseteq F$. Also for every $p \in \mathcal{P}_n$, we have $\mu_p(E) \subseteq \mu_n(E) \subseteq F$. So, the extension E/F is n -pure. Hence by Lemma 3.5.37, we have that E/F is a G -Cogalois extension. □

Theorem 3.5.41. *Let F be a field, and let $r, n \in \mathbb{N}^*$, $a_1, \dots, a_r \in F^*$. Let's denote $G = F^* \langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle$ and we have $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$. If $\gcd(n, e(F)) = 1$, and $\mu_n(E) \subseteq F$, then the following statements hold.*

- (1) *The generalized n -Kummer extension E/F is G -Cogalois.*
- (2) *The maps $H \longrightarrow F(\sqrt[n]{H} \cap G)$ and $K \longrightarrow K^n \cap (F^{*n} \langle a_1, \dots, a_r \rangle)$ establish isomorphisms of lattices, inverse to one another, between the lattice of all subgroups H of $F^{*n} \langle a_1, \dots, a_r \rangle$ containing F^{*n} and the lattice of all intermediate fields K of E/F . Moreover, any subextension K/F of E/F is a generalized n -Kummer extension.*
- (3) *If H is any subgroup of $F^{*n} \langle a_1, \dots, a_r \rangle$ containing F^{*n} , then any set of representatives of the group $(\sqrt[n]{H} \cap G)/F^*$ is a vector space basis of $F(\sqrt[n]{H} \cap G)$ over F , and $[F(\sqrt[n]{H} \cap G) : F] = |H/F^{*n}|$. In particular, one has*

$$[E : F] = |F^{*n} \langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle / F^*| = |F^{*n} \langle a_1, \dots, a_r \rangle / F^{*n}|.$$

□

Proposition 3.5.42. *A finite generalized Kummer extension is a classical Kummer extension if and only if it is a Galois extension.*

Proof. Assume that E/F is a finite generalized n -Kummer extension, where we have $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$, $r \in \mathbb{N}^*$, $a_1, \dots, a_r \in F^*$, and $\mu_n(E) \subseteq F$. Now we denote $G = F^* \langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle$ and let $m = \exp(G/F^*)$. If E/F is a Galois extension, then by Corollary 3.5.29, we have $\gcd(m, e(F)) = 1$ and $\zeta_m \in E$. Since $m | n$, we have

$$\zeta_m \in E \cap \mu_m(\Omega) = \mu_m(E) \subseteq \mu_n(E) \subseteq F.$$

Hence, E/F is a classical m -Kummer extension.

Conversely, we know that any classical Kummer extension is a Galois extension by definition.

□

Remark 3.5.43. Let E/F be an extension such that there exists $r, n_1, \dots, n_r \in \mathbb{N}^*$ and $a_1, \dots, a_r \in F^*$ with $E = F(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$. Let $G = F^*\langle \sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r} \rangle$ and $n = \text{lcm}(n_1, \dots, n_r)$. Now we show that if $\gcd(e(F), n) = 1$, and $\mu_n(E) \subseteq F$, then E/F is a generalized n -Kummer extension and a G -Cogalois extension. For all i , $1 \leq i \leq r$ we can find some $q_i \in \mathbb{N}^*$ such that $n = q_i n_i$. So we have $\sqrt[n]{a_i} = \sqrt[q_i]{a_i^{q_i}}$, and $E = F(\sqrt[q_1]{c_1}, \dots, \sqrt[q_r]{c_r})$, where $c_i = a_i^{q_i}$, for all i , $1 \leq i \leq r$. Hence by Lemma 3.5.40, E/F is a $F^*\langle \sqrt[q_1]{c_1}, \dots, \sqrt[q_r]{c_r} \rangle$ -Cogalois extension. \square

Examples 3.5.44. (1) A generalized Kummer extension is not necessarily a classical Kummer extension. Consider the extension E/F , where $F = \mathbb{Q}(i)$, and $E = F(\sqrt[8]{3})$. So, $e(F) = 1$. Clearly, $\gcd(8, 1) = 1$ and $\mu_8(E) = \{1, -1, i, -i\} \subseteq F$, since $\sqrt{2} \notin E$. So, by Remark 3.5.43, we have that E/F is a generalized 8-Kummer extension, since $\text{lcm}(2, 8) = 8$. The minimal polynomial over F of $\sqrt[8]{3}$, which is, $X^8 - 3$ does not split over E , since $\sqrt{2} \notin E$. So, E/F is not a normal extension, hence it is not a Galois extension. So, by Proposition 3.5.42, E/F is not a classical Kummer extension.

(2) Notice that any generalized n -Kummer extension E/F is clearly n -pure since for any $p \in \mathcal{P}_n$, we have $\mu_p(E) \subseteq \mu_n(E) \subseteq F$. However the converse does not hold. Consider the extension $\mathbb{Q}(\zeta_{p^3})/\mathbb{Q}(\zeta_p)$, where p is an odd prime. We claim that this extension is p^2 -pure but not a generalized p^2 -Kummer extension. Let $E = \mathbb{Q}(\zeta_{p^3})$, and $F = \mathbb{Q}(\zeta_p)$. Firstly, we have to show that for all $p \in \mathcal{P}_{p^2}$, $\mu_p(E) \subseteq F$. We have $\mathcal{P}_{p^2} = \{p\}$. But clearly $\mu_p(E) \subseteq F$. So, E/F is p^2 -pure. But E/F is not a generalized p^2 -Kummer extension, since $\mu_{p^2}(E) \not\subseteq F$. \square

Kummer Extensions with Few Roots of Unity

In this subsection we are going to present a very particular cases of generalized Kummer extensions, namely the Kummer extensions with few roots of unity.

Definition 3.5.45. A finite extension E/F is said to be an n -Kummer extension with few roots of unity, where $n \in \mathbb{N}^*$, if $\gcd(n, e(F)) = 1$, $\mu_p(E) \subseteq \{-1, 1\}$, and there exists $r \in \mathbb{N}^*$, and $a_1, \dots, a_r \in F^*$ such that $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$.

A Kummer extension with few roots of unity is an extension which is an n -Kummer extension with few roots of unity for some positive integer $n \geq 1$. \square

The following result is a consequence of Theorem 3.5.41.

Theorem 3.5.46. *Let F be a field, and let $r, n \in \mathbb{N}^*$, $a_1, \dots, a_r \in F^*$. Let's denote $G = F^* \langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle$ and we have $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$. If $\gcd(n, e(F)) = 1$, and $\mu_n(E) \subseteq \{-1, 1\}$, then the following statements hold.*

- (1) *The n -Kummer extension with few roots of unity E/F is G -Cogalois.*
- (2) *The maps $H \longrightarrow F(\sqrt[n]{H} \cap G)$ and $K \longrightarrow K^n \cap (F^{*n} \langle a_1, \dots, a_r \rangle)$ establish isomorphisms of lattices, inverse to one another, between the lattice of all subgroups H of $F^{*n} \langle a_1, \dots, a_r \rangle$ containing F^{*n} and the lattice of all intermediate fields K of E/F . Moreover, any subextension K/F of E/F is an n -Kummer extension with few roots of unity.*
- (3) *If H is any subgroup of $F^{*n} \langle a_1, \dots, a_r \rangle$ containing F^{*n} , then any set of representatives of the group $(\sqrt[n]{H} \cap G)/F^*$ is a vector space basis of $F(\sqrt[n]{H} \cap G)$ over F , and $[F(\sqrt[n]{H} \cap G) : F] = |H/F^{*n}|$. In particular, one has*

$$[E : F] = |F^{*n} \langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle / F^*| = |F^{*n} \langle a_1, \dots, a_r \rangle / F^{*n}|.$$

\square

Remark 3.5.47. (1) Let F be a subfield of \mathbb{R} , and let $r, n \in \mathbb{N}^*$, $a_1, \dots, a_r \in F^*$. Denote $G = F^* \langle \sqrt[n]{a_1}, \dots, \sqrt[n]{a_r} \rangle$ and $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$. If $\gcd(n, e(F)) = 1$, and $\mu_n(E) \subseteq \{-1, 1\}$, then (1), (2), (3) of Theorem 3.5.46 is satisfied, since any subfield of \mathbb{R} is a field with few roots of unity.

(2) Consider the extension $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}(\sqrt{-3})$. Let $E = F(\sqrt[3]{2})$, where we have $F = \mathbb{Q}(\sqrt{-3})$. Our aim is to show that this extension is a classical Kummer extension which is not a Kummer extension with few roots of unity. E/F is a Galois extension since it is a splitting field of the separable polynomial $X^3 - 2 \in F[X]$.

Also by Proposition 2.6.5, $\text{Gal}(E/F) \cong \mathbb{Z}_3$, since the degree of this extension is 3. So, we have an Abelian extension. Now we claim that this extension is a classical 3-Kummer extension. Clearly, $\gcd(3, 1) = 1$, and $\mu_3(\Omega) \subseteq F$. Also $\text{Gal}(E/F)$ is a group of exponent 3. Hence, the extension E/F is a classical 3-Kummer extension. But this extension is not a Kummer extension with few roots of unity, since $\mu_3(E) \not\subseteq \{-1, 1\}$. E/F , being a classical Kummer extension, is an $F^*\langle\sqrt[3]{2}\rangle$ -Cogalois extension by Theorem 3.5.38. So, E/F is an Abelian $F^*\langle\sqrt[3]{2}\rangle$ -Cogalois extension. Hence by Theorem 3.5.30, the groups $\text{Gal}(E/F)$ and $\text{Kne}(E/F)$ are isomorphic. Thus,

$$\text{Gal}(E/F) \cong \text{Kne}(E/F) \cong \mathbb{Z}_3.$$

□

Quasi Kummer Extensions

In this subsection we are going to deal with another class of G -Cogalois extensions, namely the class of quasi-Kummer extensions. These extensions are close to the class of classical Kummer extensions.

Definition 3.5.48. A finite extension E/F is said to be a quasi-Kummer extension, if there exists $r, n_1, n_2, \dots, n_r \in \mathbb{N}^*$, and $a_1, \dots, a_r \in F^*$ such that $E = F(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$, $\gcd(n, e(F)) = 1$, and $\mu_p(\Omega) \subseteq F$ for any $p \in \mathcal{P}_n$, where $n = \text{lcm}(n_1, \dots, n_r)$. □

Clearly, any finite classical Kummer extension is a quasi-Kummer extension. But the converse is not true, since the class of quasi-Kummer extensions is strictly larger than the class of classical Kummer extensions.

Theorem 3.5.49. A quasi-Kummer extension $F(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})/F$ as in the Definition 3.5.48, is $F^*\langle\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r}\rangle$ -Cogalois. □

Proof. Let $G = F^*\langle\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r}\rangle$, $n = \text{lcm}(n_1, \dots, n_r)$, and $m = \exp(G/F^*)$. Then clearly, $m \mid n$. So, for any $p \in \mathcal{P}_m$, $p \mid n$, and we have $\mu_p(E) \subseteq \mu_p(\Omega) \subseteq F$. Hence, the extension E/F is m -pure. Also this extension is separable by Corollary 3.5.26, hence by Theorem 3.5.16, E/F is G -Cogalois. □

Theorem 3.5.50. *Any finite Galois G -Cogalois extension is a quasi-Kummer extension.*

Proof. Let E/F be a finite Galois G -Cogalois extension, and let $\{b_1, \dots, b_r\}$ be a set of representatives of the finite quotient group G/F^* . If $n = \exp(G/F^*)$, then $b_i^n = a_i \in F$, for all i , $1 \leq i \leq r$. So, we have

$$E = F(b_1, \dots, b_r) = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r}).$$

So, E/F is a G -radical extension. We also have that E/F is a Galois extension. So, by Corollary 3.5.29 we have $\gcd(n, e(F)) = 1$ and $\zeta_n \in E$. Hence, $\mu_n(\Omega) \subseteq \mu_n(E)$. By Theorem 3.5.16, the G -Cogalois extension E/F is n -pure. So for all $p \in \mathcal{P}_n$, $\mu_p(E) \subseteq F$. Thus, $\mu_p(\Omega) \subseteq \mu_p(E) \subseteq F$, for all $p \in \mathcal{P}_n$. But this implies that the extension E/F is quasi-Kummer. \square

Corollary 3.5.51. *The following assertions are equivalent for an algebraic number field E .*

- (1) E/\mathbb{Q} is a Galois G -Cogalois extension for some group G .
- (2) E/\mathbb{Q} is an Abelian G -Cogalois extension for some group G .
- (3) There exists finitely many nonzero rational integers a_1, \dots, a_r such that $E = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_r})$.
- (4) E/\mathbb{Q} is a classical 2-Kummer extension.

Proof. (1) \implies (3) : By Theorem 3.5.50, E/\mathbb{Q} is a quasi-Kummer extension. So, there exists $r, n_1, \dots, n_r \in \mathbb{N}^*$, and $a_1, \dots, a_r \in \mathbb{Q}^*$ such that $E = \mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$. Also we have $\mu_p(\mathbb{C}) \subseteq \mathbb{Q}$, for all $p \in \mathcal{P}_n$, where $n = \text{lcm}(n_1, \dots, n_r)$. But we know that $\zeta_m \in \mathbb{Q}$ if and only if $m = 1$ or $m = 2$. So, we must have that $n \leq 2$. But this implies that $n_i \leq 2$, for all $i = 1, \dots, r$. So, we are done.

(3) \implies (4) follows from Corollary 3.5.36.

(4) \implies (2) and (2) \implies (1) are obvious. \square

Remark 3.5.52. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is G -Cogalois for some group G if and only if $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. We know that

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U(\mathbb{Z}_n),$$

where $U(\mathbb{Z}_n)$ denotes the group of units of the ring \mathbb{Z}_n of integers modulo n . Also we know that the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension, since $\mathbb{Q}(\zeta_n)$ is a splitting field of the separable polynomial $X^n - 1 \in \mathbb{Q}[X]$. So, for $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$, the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an Abelian G -Cogalois extension for some group G . So, by Theorem 3.5.30, we have that the groups $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $\text{Kne}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ are isomorphic. So,

$$\text{Kne}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U(\mathbb{Z}_n).$$

□

BIBLIOGRAPHY

- [1] T. ALBU, “*Cogalois Theory*”, Marcel Dekker, Inc., Basel New York, pp. 15-104, 2003.
- [2] T. ALBU and F. NICOLAE, “Kneser Field Extensions with Cogalois Correspondence”, *J. Number Theory*, **52** (1995), 299-318.
- [3] T. ALBU and F. NICOLAE, “ G -Cogalois Field Extensions and Primitive Elements” in “Symposia Gaussiana”, Conference A: Mathematics and Theoretical Physics, Eds. M. Behara, R. Fritsch, and R.G. Lintz, Walter de Gruyter & Co., Berlin New York, 1995, pp. 233-240.
- [4] T. ALBU and F. NICOLAE, “Heckesche Systeme Idealer Zahlen und Knesersche Körpererweiterungen”, *Acta Arith.* **73** (1995), 43-50.
- [5] T. ALBU and F. NICOLAE, “Finite Radical Field Extensions and Crossed Homomorphisms”, *J. Number Theory* **60** (1996), 291-309.
- [6] T. ALBU and F. NICOLAE, and M. ȚENA, “Some Remarks on G -Cogalois Field Extensions”, *Rev. Roumaine Math. Pures Appl.* **47** (2002).
- [7] F. BARRERA-MORA, M. RZEDOWSKI-CALDERÓN and VILLA-SALVADOR, “On Cogalois Extensions”, *J. Pure Appl. Algebra* **76** (1991), 1-11.
- [8] L. GAAL, “*Classical Galois Theory*”, AMS Chelsea Publishing Company, USA, pp. 99-108 & pp. 114-116, 1998.
- [9] C. GREITHER and D.K. HARRISON, “*A Galois Correspondence for Radical Extensions of Fields*”, *J. Pure Appl. Algebra* **43** (1986), 257-270.

-
- [10] N. JACOBSON, “*Basic Algebra I*”, W. H. Freeman and Company, San Francisco, pp. 204-248, 1974.
- [11] I. KAPLANSKY, “*Fields and Rings*” (2nd ed.), The University of Chicago Press, Chicago, pp. 2-55, 1972.
- [12] M. KNESER, “Lineare Abhängigkeit von Wurzeln”, *Acta Arith.* **26** (1975), 307-308.
- [13] J. ROTMAN, “*Galois Theory*”, Springer-Verlag, Barcelona Berlin Budapest Heidelberg Hong Kong London New York Paris Tokyo, pp. 19-20 & pp. 28-33, 1990.
- [14] I. STEWART, “*Galois Theory*” (3rd ed.), Chapman and Hall/CRC, Boca Raton London New York Washington D.C, pp. xxiii-xxxv, 2004.

VITA

HATİCE BOYLAN was born in Konya, Turkey on December 11, 1979. She received her B.Sc. degree in Mathematics from Boğaziçi University, İstanbul, in 2003. From September 2003 to June 2005, she worked as a teaching and research assistant in Koç University, Turkey and had completed her masters degree in this university.

