Kingdom of Saudi Arabia

Imam Mohammad Ibn Saud Islamic University

College of Science

Department of Mathematics and Statistics

Master of Science in Mathematics

Research Project Report

(MAT699)

title:

Galois Theory and Insoulablitiy of The Quintic Equation by Radicals

Presented by

Sara Saeed bin Haif

Supervised by:

Prof. Mohammed Alkadhi

Second Semester 1439-1440

Dedication

إهداء

إلى من كلله الله بالهيبة والوقار، إلى من علمني العطاء بدون انتظار، إلى من أحمل اسمه بكل افتخار، أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول انتظار وستبقى كلماتك نجوم أهتدي بها اليوم وفي الغد وإلى الأبد.

إلى والدي العزيز

إلى ملاكي في الحياة، إلى معنى الحب والتفاني، إلى بسمة الحياة وسرها، إلى من كان دعاؤها سر نجاحي وحنانها بلسم جراحي إلى أغلى الأحباب.

إلى أمي الغالية

إلى من عليه أعتمد، إلى الشمعة المتقدة التي تنير ظلمة حياتي، إلى من بوجودها أكتسب قوة لا حدود لها

إلى أختي الحبيبة

إلى رفيق دربي في هذه الحياة، إلى من تطلعت إلى نجاحي بنظرات تملؤها الأمل والمحبة، أشكرك من الأعماق على مواقفك النبيلة

إلى أخي الغالي

أهدي هذا البحث لكل من ساهم في وصولي إلى هنا، إلى كل من علمني شيئاً جديداً وغذى فكري وبصيرتي، إلى كل من وقف بجانبي وساعدني في كل المصاعب

إلى أساتذتي وأستاذاتي

Acknowledgment

All praises be to Allah who enlightened my mind with science and knowledge and helped me to achieve this research. After thanking God Almighty and then my dear parents, I thank all my teachers and professors who have taught me through my educational path since my tender age, especially who have taught me at the university stage, which is a pivotal stage in my life. I also sincerely thank all those who(directly or indirectly) have contributed to this honourable educational level. Much gratitude and appreciation are given to Prof.Mohammed Al-kadhi, who made a great effort guiding me on choosing the subject of this research and providing me with suitable references and keep helping me throughout writing of this research and, in addition, helping me with editing and language issues. Also I won't forget to thank him for his nice historical introduction he made for my research. For all of this and more I express my sincere thanks to him, for without his generous guidance, this research won't be completed as it shows now.

Abstract

In this research, we give foundations of Galois Theory and its important implication on insoulability of quintic equation. In the first chapter, we lay down the background on finite extensions needed to study this subject. In the second chapter, we proceed in studying Galois theory, after some introductory results, we state and prove the Fundamental Theorem of Galois on finite field extensions. Then we conclude this chapter with the famous important result of insoulability of the quintic equation and prove it as a consequence of the Fundamental Theorem of Galois.

خلاصة البحث

في هذا البحث نعرض أساسيات (نظرية جالوا) والنتيجة المهمة المترتبة عليها باستحالة وجود قانون عام للمعادلة من الدرجة الخامسة في مجهول واحد يمكن صياغته باستخدام فقط العمليات الجبرية المعتادة وعملية الجذور من أي رتبة. في الفصل الأول نبني الخلفية الرياضية اللازمة لدراسة نظرية جالوا في امتدادات الحقول الجبرية. أما في الفصل الثاني والذي يمثل لب هذا البحث فنباشر في دراسة نظرية جالوا حيث بعد عرض بعض النتائج المهمة الضرورية نعرض نظرية جالوا الأساسية للامتدادات المنتهية للحقول. و أخيراً نختم هذا الفصل بالنتيجة المهمة التاريخية حول استحالة حل المعادلة من الدرجة الخامسة ونثبتها كنتيجة من نظرية جالوا الأساسية.

Contents

Introduction

First, we give a historical survey of this fascinating thoery and pivotal subject of "Galois Theory". It is needless to say that Geometry and Numbers are the two foundations on whom mathematics was built on from the evolve of human civilizations. The first deep and most important subject in all fields of mathematics is solving equations on one unknown which has a long and rich history of developments. The solution of the linear equation was known from untiquity In the 9^{th} century Muhammad ibn Musa Al-Khwarizmiy(780-850) gave the procedures of solving the general second degree equation in his famous book "Aljabr wa Almugabla".

For the general 3^{rd} and 4^{th} degree equations, they were difficult to deal with and their solutions became a formidable tasks and they were finally solved through the period 1535-1545 in a dramatic series of events by Firro, Fontana, Cardano, and Ferrari.

For the quintic equations, i.e. the 5^{th} degree equation in one unknown; since the 16^{th} century the mathematician were struggling finding the general law of solving this equation by radicals. As the time went without any sign of finding this seeked solution, some mathematicians start to doubt that is there ever a solution of this equation. Among those was the famous mathematician Joseph Lagrange(1736-1813) who even though didn't succeeded in proving the impossibility of solving quintic by radicals, he paved the way for next explorers seeking this proof. After failure of many mathematicians in finding the proof of this impossibility, Neils Abel(1802-1829) succeeded in providing the first complete proof of the impossibility of solving the general quintic equation by radicals. Abel's proof was later superceded by the more elegant and comprehensive proof of Evariste Galois in 1830. Both Abel and Galois lived a miserable lives and died too early. Their profounding proofs remained unnoticed until the fourties of the 19^{th} century, moreover, the great impact of Galois proof and method was not realized until the end of 19^{th} century.

Now we come the to material of this thesis which consists of two chapters. In the first

chapter, we lay down the necessary background in algebraic field extensions which is needed for studying Galois theory on finite extension fields. We study in this chapter the notions of algebraic, splitting, separable, and normal extensions and introduce some of their basic properties. In the second chapter which represents the core material of this research, we define the Galois group of any finite field extensions $(K : F)$ and study some of its properties regarding the dimension $[K : F]$ and we prove the main result showing the order of the Galois group $\Gamma(K : F)$ equals $[K : F]$ if and only if K is normal and separable over F. Next after giving some other properties of these kinds of field extensions, we state and prove the main theorem of this research the(Fundamental Theorem of Galois) which gives a one-one corresponding between intermediate subfields of a normal separable extension field $(K : F)$ and the subgroups of its Galois group $\Gamma(K : F)$ with several important results. Finally in the last section we use Galois theory to show the important result of insolvability of the general quintic equation by radicals which was the main factor in evolving of Galois Theory. We start this section by defining radical extension fields and reviewing the important notion of solvable groups (this notion came out as a result of trying to solve the quintic equations by radicals). Next we state and prove the important theorem which related the solvability of Galois group with corresponding field extension being a radical extension. After that we state and prove the impossiblity of solving the general quintic equation by radicals by considering a specific 5^{th} degree equation over the field of rational numbers whose Galois group is not solvable, i.e., no splitting field of this polynomial would be contained in a radical extension field of the rational numbers.

Chapter1

Finite Algebraic Extensions

Throughout this research, $F \subset K$ are fields and we denote this by $K : F$ and call it an *extension field*. If $\dim K_F$ is finite we call it a *finite extension* and denote $\dim K_F$ by $[K : F]$.

All results in sections 1 and 2 of this chapter are standard in any first Algebra graduate course, so we won't give proofs of these results but we refer the reader to references [1] and [2].

1.1 Basics

(1.1) Definition.

Let $K : F$ and $L : F$ be field extensions. An F-*homomorphism* $\varphi : K \longrightarrow L$ is a homomorphism of fields such that $\varphi(a) = a$ for all $a \in F$. An F-*embedding* is an injective F-homomorphism. An F-*isomorphism* is a bijective F-homomorphism. An F-*automorphism* of K is an F-isomorphism mapping K onto itself. Two extensions K:F and L:F of a field F are said to be F-*isomorphic* if there is an F-isomorphism $\varphi : K \longrightarrow L$.

(1.2) Proposition (**The Tower Law**)**.**

Let L:K and K:F be field extensions. Then:

$[L : F]$ is finite if and only if $[L : K]$ and $[K : F]$ are finite.

In this case, $[L : F] = [L : K][K : F]$.

(1.3) Definition.

Let K:F be a field extension and let $\alpha \in K$. α is called *algebraic* over F if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. If α is not algebraic over F, we call it *transcendental* over F. If every element of K is algebraic over F, then we say that K is *algebraic* over F and we call the K:F an *algebraic* extension.

(1.4) Proposition.

Any finite field extension is algebraic over the basic field.

(1.5) Proposition.

Let K:F be an extension field and let $\alpha \in K$ be algebraic over F. Then there exists a unique irreducible monic polynomial - i.e. its leading coefficient is one - $p(x) \in F[x]$ such that $p(\alpha) = 0$. Moreover, if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x)|f(x)$.

(1.6) Definition.

If $\alpha \in K$ is algebraic over F, we call the polynomial $p(x)$ above the *minimal polynomial* of α over F and denote it by $p_\alpha(x)$.

(1.7) Proposition.

Let K:F be a field extension and let $\alpha \in K$ be an algebraic over F. Then $[F(\alpha)$:$F]$ is finite and it equals the $\deg(p_\alpha(x))$.

(1.8) Proposition.

A field extension K:F is finite if and only if there exists a finite set of algebraic elements $\alpha_1, \alpha_2, ..., \alpha_n$ in K such that K=$F(\alpha_1, \alpha_2, ..., \alpha_n)$.

(1.9) Proposition.

Let L:K and K:F be field extensions. Then L:F is an algebraic field extension if and only if L:K and K:F are both algebraic field extensions.

1.2 Splitting Fields

(2.1) Definition.

Let K:F be a field extension. A non-zero $f(x) \in F[x]$ is said to *split* in K if it is a constant polynomial or there exist elements $c, \alpha_1, \alpha_2, ..., \alpha_n \in K$ such that $f(x) = c(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$, i.e., $f(x)$ can be factored into linear factors in $K[x]$.

(2.2) Theorem (Kronecker).

Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there exists an extension field K and an element α of K such that $f(\alpha) = 0$.

(2.3) Proposition.

Let K:F be a field extension and let $\alpha, \beta \in K$ be algebraic over F. Then $F(\alpha)$ is isomorphic to $F(\beta)$ if and only if α and β have the same minimal polynomial over F.

(2.4) Definition.

Let K:F be a field extension and let $f(x)$ be a non-constant polynomial in $F[x]$. We call the field K a *splitting field* for f over F if the following holds

(i) The polynomial f splits in K over F.

(ii) The polynomial f does not split over any proper subfield of K containing F.

(2.5) Proposition.

Let K:F be a field extension and let $f(x) \in F[x]$ which splits in K. Then there is a unique splitting subfield (up to F-isomorphism) of $f(x)$ in K.

For the field extension $\mathbb{C}$:$\mathbb{Q}$, the Fundamental Theorem of Algebra asserts that a non-constant polynomial $f(x) \in \mathbb{Q}[x]$ always splits in the field $\mathbb{C}$.

Note that if a polynomial $f(x)$ splits in an extension field K of F and if α_1,α_2,...α_n are the zeros of this polynomial in K, then the *unique splitting field* ,up to an F-isomorphism, of f over F contained in K is exactly the field $F(\alpha_1, \alpha_2, ..., \alpha_n)$ obtained by adjoining the zeros of f to F.

1.3 Normal and Separable Extensions

(3.1) Definition.

A field extension K:F is called *normal* if every irreducible polynomial in $F[x]$ having a zero in K splits in K.

So we can see from definition above that: a finite field extension K:F is normal if and only if for any element $\alpha \in K$, the minimal polynomial $p(x) \in F[x]$ of α in K splits in K.

(3.2) Proposition.

Let K:F be a field extension. Then K is a splitting field over F for some polynomial $f(x) \in F[x]$ if and only if the field extension K:F is both finite and normal.

Proof.

Assume that K:F is both finite and normal. Then by proposition(1.8), there exist α_1,α_2,...,α_n in K such that K=$F(\alpha_1,\alpha_2,...,\alpha_n)$ where α_i's are algebraic over F. Now let $p_i(x) \in$ F[x] be the minimal polynomial of α_i in F for each i=1,2,...,n, and let $f(x) = p_1(x)p_2(x)...p_n(x)$. Since K:F is normal, $p_i(x)$ splits in K for i=1,2,...,n. Hence f splits in K. Moreover, K is generated by α_1,α_2,...,α_n which implies that K is the splitting field of f over F.

Conversely, suppose that K is a splitting field for some polynomial $f(x) \in F[x]$. Then K is generated by the zeros of f. Using proposition(1.8), K:F is finite. For the normality, let $g(x) \in F[x]$ be irreducible, and let L be a splitting field of fg over K. Then each of $f(x)$ and $g(x)$ splits in L. Now suppose that α and β are zeros of $g(x)$ in L. Then $f(x)$ splits in

both $K(\alpha)$ and $K(\beta)$. So if $f(x)$ splits in any subfield E of L containing $F(\alpha)$, then $K \subset E$ and hence $K(\alpha) \subset E$. Hence $K(\alpha)$ is a splitting field of $f(x)$ over $F(\alpha)$. Similarly, we found that $K(\beta)$ is a splitting field of $f(x)$ over $F(\beta)$.

Now define the mapping $\varphi : F(\alpha) \longrightarrow F(\beta)$ by $\varphi(h(\alpha)) = h(\beta)$ for all $h(x) \in F[x]$. So φ is well-defined mapping, since for any two polynomials $h_1(x)$ and $h_2(x)$ in $F[x]$ having the same value at some zero of $g(x)$ if and only if $h_1 - h_2$ is divisible by g. Since $K(\alpha)$ and $K(\beta)$ are splitting fields of $f(x)$ over $F(\alpha)$ and $F(\beta)$ respectively, we can extend φ to an F-isomorphism $\varphi^* : K(\alpha) \longrightarrow K(\beta)$. Therefore $K(\alpha)$ and $K(\beta)$ are F-isomorphic, hence $[K(\alpha) : F] = [K(\beta) : F]$. By Tower Law, $[K(\alpha) : F] = [K(\alpha) : K][K : F]$ and $[K(\beta) : F] = [K(\beta) : K][K : F]$. Thus$[K(\alpha) : K] = [K(\beta) : K]$. Hence $\alpha \in K$ if and only if $\beta \in K$. So for any irreducible polynomial in $F[x]$ having a zero in K must split in K. It follows that, $K : F$ is normal. $\square$

(3.3) Example.

Let K be a splitting field of $x^3 - 2$. Then

$$x^3 - 2 = (x - u)(x - \omega u)(x - \omega^2 u)$$

where $u = \sqrt[3]{2}$ and $\omega = (-1 + \sqrt{-3})/2$. Clearly $K = \mathbb{Q}(u, \omega)$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, $\omega \notin \mathbb{Q}(u)$, and $u \notin \mathbb{Q}(\omega)$. By proposition(3.2), K is normal. Note that $[\mathbb{Q}(u) : \mathbb{Q}] = 3 = [\mathbb{Q}(u, \omega) : \mathbb{Q}(\omega)]$, since the minimal polynomial of u has degree 3 over $\mathbb{Q}$ and $\mathbb{Q}(\omega)$. Also $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, since the minimal polynomial of ω is $(x-\omega)(x-w^2)$ and has degree 2 over $\mathbb{Q}$. Now by Tower Law $[K : \mathbb{Q}] = [K : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 3 \times 2 = 6$. However, neither $\mathbb{Q}(u)$ nor $\mathbb{Q}(\omega)$ is a splitting field of $x^3 - 2$ over $\mathbb{Q}$, so both of them are not normal over $\mathbb{Q}$.

It can easy shown that if $L : F$ is normal finite extension and K is an intermediate field of this extension, then so is $L : K$. But $K : F$ is not necessarily normal, e.g. in the example, $\mathbb{Q}(u : \omega) : \mathbb{Q}$ and $\mathbb{Q}(u, \omega) : \mathbb{Q}(u)$ are both normal but $\mathbb{Q}(u) : \mathbb{Q}$ is not.

(3.4) Definition.

Let F be a field and let $f(x)=\sum_{i=0}^{n} a_i x^i \in F[x]$. The *formal derivative* f' of f is defined by $f'(x)=\sum_{i=0}^{n} i a_i x^{i-1}$.

It is easy to show that $\forall f(x), g(x) \in F[x]$, $(f+g)' = f' + g'$ and $(fg)' = f'g + fg'$ If f is constant polynomial, then $f'=0$.

(3.5) Proposition.

Let F be a field and let $f(x) \in F[x]$. Then the polynomial f has a repeated zero in some splitting field of f over F if and only if there is $g(x) \in F[x]$ of positive degree such that $g(x) | f(x)$ and $g(x) | f'(x)$.

Proof.

If c is a repeated zero of $f(x) \in F[x]$ in some extension L, then $f(x) = (x-c)^2 h(x)$, for some polynomial $h(x) \in L[x]$. Since $f'(x) = 2(x-c)h(x) + (x-c)^2 h'$, we note that $f'(c) = 0$. Hence both $f(x)$ and $f'(x)$ have a common factor $x - c$ of positive degree in the extension L of F.

Now, assume that there exists $g(x) \in F[x]$ of positive degree such that $g(x) | f(x)$ and $g(x) | f'(x)$. Let a be a zero of $g(x)$. Then a is a zero of both $f(x)$ and $f'(x)$, and thus there exists a polynomial $p(x)$ such that $f(x) = (x-a)p(x)$. Hence $f'(x) = (x-a)p'(x) + p(x)$ and $0 = f'(a) = p(a)$. This means that $x - a$ is a factor of $p(x)$. So we showed that, $f(x) = (x-a)^2 q(x)$, where $p(x) = (x-a)q(x)$, for some polynomial $q(x) \in L[x]$. Thus a is a repeated zero of $f(x)$. $\square$

(3.6) Definition.

Let $f(x) \in F[x]$ be irreducible. $f(x)$ is called *separable* over F if there is no repeated zero for $f(x)$ in some splitting field(hence in any splitting field) of $f(x)$ over F. Any polynomial $g(x) \in F[x]$ is called *separable* over F if all its irreducible factors are separable over F, otherwise $g(x)$ is called *inseparable*.

(3.7) Definition.

Let K:F be an algebraic field extension and let $a \in K$. Then a is called *separable* if its the minimal polynomial $p_a(x) \in F[x]$ is separable over F. The field K is called *separable* extension of F if all its elements are separable over F.

(3.8) Proposition.

Let F be a field. Then an irreducible polynomial f is inseparable over F if and only if f'=0.

Proof.

Suppose that $f(x) \in F[x]$ is an irreducible inseparable polynomial. Then $f(x)$ has a repeated zero in some extension of F, so by proposition(3.5) there exists a polynomial $g(x) \in$ F$[x]$ of positive degree that divides both $f(x)$ and $f'(x)$. Since f is irreducible, $g(x) = af(x)$ for some $a \in$ F. Hence $f(x)$ divides $f'(x)$. But deg(f')$<$ deg(f). We deduce that, $f'(x) = 0$.

Conversely, suppose that $f'(x) = 0$. Then both of $f(x)$ and $f'(x)$ are divisible by $f(x)$. By proposition(3.5), we obtain that $f(x)$ has e repeated zero in some extension of F. It follows that, f is inseparable over F. □

(3.9) Proposition.

Let K:F be algebraic extension with char(F)=0 and let $f(x) \in F[x]$ be irreducible. Then:
(i) $f(x)$ is separable over F.
(ii) K is separable over F.

Proof.

(i)Suppose that $f(x)$ is not separable. Then by proposition(3.8), $f'(x) = 0$. Therefore $f(x)$ must be a constant which contradicts the irreducibility of $f(x)$. Thus $f(x)$ is separable.

(ii)Let $d \in K$ be algebraic over F with a minimal polynomial $p_d(x)$. Then by pat(i), $p_d(x)$ is separable over F. This shows that any algebraic element over F, its minimal polynomial must be separable. Hence $K : F$ is separable. □

For the corresponding proposition on finite fields, we need the following result whose proof can be found in [2].

(3.10) Proposition.

Let F be a finite field with char(F)=p, then:

$(F^*, .)$ is cyclic and $\mid F \mid = p^n$ for some $n \in \mathbb{N}$. Moreover, $F \simeq \mathbb{Z}_p(\alpha)$ for some $\alpha \in F$.

(3.11) Proposition.

Let $F = \mathbb{Z}_p(\alpha)$ be a finite field with $\mid F \mid = p^n$. Then the extension $F : \mathbb{Z}_p$ is a separable extension.

Proof.

$(F^*, .)$ is cyclic group of order $p^n - 1$ implies $\forall a \in F^*$, $a^{p^n-1} = 1$. Hence $\forall a \in F$, $a^{p^n} = a$, i.e. every element of F is a zero of the polynomial $f(x) = x^{p^n} - x$. Thus all zeros of $f(x)$ are in F and are all distinct. So $f(x)$ is separable over $\mathbb{Z}_p$, i.e. $F : \mathbb{Z}_p$ is separable. □

(3.12) Example.

Let $F = \mathbb{Z}_2(y)$ be the field of quotients of the ring $\mathbb{Z}_2[y]$ of polynomials in the indeterminate y with coefficients from $\mathbb{Z}_2$. Consider the polynomial $f(x) = x^2 - y \in F[x]$. To see that $f(x)$ is irreducible over F, it suffices to show that it has no zeros in F. Now suppose that $g(y)/h(y)$ is a zero of $f(x)$. Then $(g(y)/h(y))^2 = y$, and threfore $(g(y))^2 = y(h(y))^2$. Since $g(y), h(y) \in \mathbb{Z}_2[y]$ and char($\mathbb{Z}_2$)=2, we have $g(y^2) = yh(y^2)$. But deg($g(y^2)$) is even, whereas deg($yh(y^2)$) is odd. So, $f(x)$ is irreducible over F. Finally, since y is a constant in $F[x]$ and the char(F)=2, we have $f'(x) = 0$ so that $f(x)$ and $f'(x)$ have $f(x)$ as a common factor. So, $f(x)$ has a repeated zero in some extension of F and hence $f(x)$ is inseparable.

(3.13) Theorem (Primitive Element Theorem).

Let K:F be a finite separable extension field. Then K=$F(\alpha)$ for some $\alpha \in K$, i.e. K is a simple extension field of F.

Proof.

We have two cases.

Case1. F is finite and K is finite over F so K is finite. Hence by proposition(3.10), $K = \mathbb{Z}_p(\alpha) = F(\alpha)$ for some $\alpha \in K$.

Case2. F is infinite. We will prove the result by mathematical induction and for that it is enough to prove it for $K = F(\alpha.\beta)$. Let $f(x)$ and $g(x)$ be the minimal polynomial of α and β respectively, and let L be a splitting field of fg. Then both f and g split in L, and hence $\alpha_1, \alpha_2, ..., \alpha_r$ and $\beta_1, \beta_2, ..., \beta_s$ are the zeros of f and g ,respectively, in L with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. α_i's and β_j's are distinct, since $K : F$ is separable.

Since F is infinite, we choose an element $d \in F$ such that $d \neq (\alpha_i - \alpha)/(\beta - \beta_j)$ for any $i \geq 1$ and $j > 1$. Let $h(x) = f(\delta - dx)$, where $\delta = \alpha + d\beta$. Then $h(x) \in F(\delta)[x]$, $h(\beta_1) = h(\beta) = f(\alpha) = 0$, and $h(\beta_j) \neq 0$ for any $j > 1$, since $\alpha_i \neq \delta - d\beta_j$ for any $i \geq 1$ and $j > 1$.

Let $u(x) \in (F(\delta))[x]$ be the minimal polynomial of β over $F(\delta)$. Now $g(x) \in F[x] \subseteq (F(\delta))[x]$ with $g(\beta) = 0$, so $u(x)|g(x)$. Similarly, since $h(\beta) = 0$, $u(x)|h(x)$. In L we have $g(x) = (x - \beta_1)(x - \beta_2)...(x - \beta_s)$ with $\beta = \beta_1$ and we see above that $h(\beta_j) \neq 0, \forall j > 1$. So $u(x)$ has only one zero, namely β, in L so $u(x) = (x - \beta)^t$ for some $t \in \mathbb{N}$, hence $t = 1$ because $K \supseteq L$ is separable over F. Thus $u(x) = (x-\beta) \in (F(\delta))[x]$ which implies $\beta \in F(\delta)$. Similarly, we show $\alpha \in F(\delta)$, hence $F(\alpha, \beta) \subseteq F(\delta)$. Thus $K = F(\delta)$ and $K : F$ is a simple extension. □

(3.14) Example.

Let F be infinite field with char(F)=p - p is prime number - and let x and y be indeterminantes over F. Then we have $F(x^p, y^p) \subseteq F(x, y)$. Now the basis of $F(x, y)$ over $F(x^p, y^p)$ is $\{1, x, x^2, ..., x^{p-1}, y, y^2, ..., y^{p-1}, xy, xy^2, ..., xy^{p-1}, x^2y, x^2y^2, ..., x^2y^{p-1}, ..., x^{p-1}y, x^{p-1}y^2, ...,$ $x^{p-1}y^{p-1}\}$ so $[F(x, y) : F(x^p, y^p)] = p^2$. Furthermore, let $z \in F(x, y)$. Then $z^p \in F(x^p, y^p)$

so that $[F(x^p, y^p)(z) : F(x^p, y^p)] \leq p$. Therefore there is no primitive z such that $F(x, y) = F(x^p, y^p)(z)$. Thus $F(x, y)$ is not simple extension.

Chapter2

Galois Theory and Insolubility of The Quintic Equation by Radicals

2.1 Galois Group

(1.1) Definition.

The *Galois group* $\Gamma(K : F)$ of a field extension K:F is the group of all F-automorphisms of K which fix elements of F, i.e. $\forall\sigma \in \Gamma(K : F)\ \forall a \in F : \sigma(a) = a$.

(1.2) Proposition.

If K:F is finite separable extension, then $|\Gamma(K : F)| \leq [K : F]$

Proof.

By Primitive Element Theorem, there exists an element $\alpha \in K$ such that $K = F(\alpha)$. Now let $\beta \in K$. Then for some polynomial $g(x) \in F[x]$, we have $\beta = g(\alpha)$. Since the coefficients of g are fixed by any F-automorphism $\phi \in \Gamma(K{:}F)$, we get $\phi(\beta) = \phi(g(\alpha)) = g(\phi(\alpha))$. This implies that, each F-automorphism ϕ is uniquely determined once $\phi(\alpha)$ is known.

Let $f(x) \in F[x]$ be the minimal polynomial of α over F. Then $f(\phi(\alpha)) = \phi(f(\alpha)) =$

0,$\forall\phi \in \Gamma(K{:}F)$, since the coefficients of f belong to F and therefore are fixed by ϕ. Hence $\phi(\alpha)$ is a zero of f. It follows that, the order of $\Gamma(K{:}F)$ is bounded above by the number of zeros of f that are in K. But the number of zeros of f are equal to deg(f)=$[K{:}F]$, since the zeros of f are all distinct and f is the minimal polynomial of α in K over F. Thus $|\Gamma(K{:}F)|\leq[K{:}F]$. $\square$

(1.3) Example.

Let $a = \sqrt[3]{2}$ and consider the extension field $\mathbb{Q}(a) : \mathbb{Q}$. Let φ be any $\mathbb{Q}$-automorphism of $\mathbb{Q}(a)$. Then it is easy to see that $\varphi(m) = m\ \forall m \in \mathbb{Z}$ and consequently $\forall\frac{m}{n} \in \mathbb{Q}\ \varphi(\frac{m}{n}) = \frac{m}{n}$.. Hence,

$$(\varphi(a))^3 = \varphi(a^3) = \varphi(2) = 2,$$

thus $\varphi(a) = a$ and consequently $\varphi(p) = \forall p \in \mathbb{Q}(a)$ Therefore, $\Gamma(\mathbb{Q}(a) : \mathbb{Q}) = \{\iota\}$ and $|\Gamma(\mathbb{Q}(a) : \mathbb{Q})| < [\mathbb{Q}(a) : \mathbb{Q}]$.

(1.4) Definition.

Let G be a group of automorphisms of a field K. Then the *fixed field* of G is the subfield F_G of K defined by

$$F_G = \{a \in K : \varphi(a) = a, \forall\varphi \in G\}.$$

(1.5) Proposition.

Let K be a field and G be a finite group of automorphisms of K. Let $F = F_G$ be the fixed field of G. Then $\forall\alpha \in K$, α is algebraic over F and the minimal polynomial $p_\alpha(x)$ can be written in the linear form $p_\alpha(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$ for some distinct elements $\alpha_1, \alpha_2, ..., \alpha_n \in K$ with $\alpha_i = \sigma_i(\alpha)$ for some $\sigma_i \in G$ and $\alpha_1 = \alpha$. Thus K is normal over F.

Proof.

Let $f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \in K[x]$. Clearly $f(\alpha) = 0$ and $\forall\sigma \in G$, $\sigma(f(x)) = f(x)$. Thus $f(x) \in F[x]$ and so α is algebraic over F. Now let $g(x) \in F[x]$ with $g(\alpha) = 0$.

Then $\forall \alpha_i$, $i = 1, 2, ..., n$, $g(\alpha_i) = \sigma_i(g(\alpha)) = 0$, since $g(x) \in F[x]$. Thus all zeros of $f(x)$ are zeros of $g(x)$. Hence $f(x)|g(x)$. So $f(x) = p_\alpha(x)$. Also $\forall i, j = 1, 2, ..., n : \alpha_i = \alpha_j$ if and only if $\sigma_i(\alpha) = \sigma_j(\alpha)$. This implies that, $\sigma_j^{-1}(\sigma_i(\alpha)) = \alpha$ if and only if $\sigma_j^{-1}(\sigma_i) = \iota$. It follows that, $\sigma_j = \sigma_i$. That is $\forall i \neq j : \sigma_j \neq \sigma_i$, hence $p_\alpha(x)$ is separable. $\square$

(1.6) Definition.

An extension $K : F$ is called *Galois extension* if K is a finite normal separable extension of F.

(1.7) Proposition.

Let $K : F$ be a finite extension field and let G be a subgroup of $\Gamma(K : F)$ such that $F = F_G$. Then $K : F$ is a Galois extension and $G = \Gamma(K : F)$. Moreover, $|G| = [K : F]$.

Proof.

By proposition(1.5), $\forall \alpha \in K$ the minimal polynomial of α over F $p_\alpha(x)$ splits in K and it is separable so $K : F$ is normal and separable. Now K is a finite algebraic extension so $K = F(\beta)$ for some $\beta \in K$ with minimal polynomial $p_\beta(x) = (x - \beta_1)(x - \beta_2)...(x - \beta_n)$ where $\beta_1 = \beta$. As we saw in proposition(1.5), $\forall i = 1, 2, ..., n$, $\beta_i = \sigma_i(\beta)$ for some $\sigma_i \in G$ and $\beta_i \neq \beta_j$, $\forall i \neq j$. So $|G| \geq n$ Hence we have by proposition(1.2), $[K : F] = n \leq |G| \leq |\Gamma(K : F)| \leq [K : F]$. Thus $G = \Gamma(K : F)$ and $|G| = [K : F]$. $\square$

(1.8) Proposition.

Let $K : F$ be a finite extension field. Then $|\Gamma(K : F)|$ divides $[K : F]$. Moreover,
$|\Gamma(K : F)| = [K : F]$ if and only if $K : F$ is a Galois extension.

Proof.

Let $G = \Gamma(K : F)$ and let $M = F_G$. Then by proposition(1.7), $K : M$ is a Galois extension with $|G| = [K : M]$. Now by Tower Law, $[K : F] = [K : M][M : F] = |G|[M : F]$. So $|G|$ divides $[K : F]$.

Suppose now $|G| = [K : F]$, then from Tower equality above $[M : F]$=1, and hence $M = F$. But $K : M$ is a Galois extension, i.e. $K : F$ is a Galois extension.

Conversely, suppose that $K : F$ is a Galois extension. Then by Primitive Element Theorem, $K = F(\alpha)$ for some $\alpha \in K$ with $\deg(p_\alpha(x))$=n=$[K : F]$.As we saw in proof of proposition(1.5) n $\leq |G|$, and by proposition(1.2) n $\leq |G| \leq [K : F]$=n. Thus $|G| = [K : F]$. □

(1.9) Proposition.

Let $K : F$ be an extension field and let M be an intermediate field of this extension. Suppose that K:F is a Galois extension, then so is K:M. Moreover, if M:F is normal extension, then M:F is a Galois extension.

Proof.

Let $\alpha \in K$ and let $f_\alpha(x)$ and $m_\alpha(x)$ be the minimal polynomials of α over F and M respectively. Then $f_\alpha(x)$ splits in K and its zeros are all distinct, since $K : F$ is a Galois extension. But $m_\alpha(x)|f_\alpha(x)$, because the coefficients of $f_\alpha(x)$ are in M and $f(\alpha) = 0$. Therefore $m_\alpha(x)$ splits in K and hence its zeros are distinct. We deduce that, $K : M$ is a Galois extension.

Now suppose that $M : F$ is a normal extension. Then clearly M:F is a separable extension, since $K : F$ is a separable extension. It follows that, $M : F$ is a Galois extension. □

2.2 The Fundamental Theorem of Galois

(2.1) Proposition.

Let $L : F$ be a Galois extension and let K be an intermediate field of this extension. Then the extension $K : F$ is normal if and only if $\phi(K) = K, \forall \phi \in \Gamma(L : F)$

Proof.

Let $\alpha \in L$ and let $f(x)$ be the minimal polynomial of α over F. If $K : F$ is normal, then f splits in K.Now for any element $\phi \in \Gamma(L : F)$, we have $0 = \phi(f(\alpha)) = f(\phi(\alpha))$, so $\phi(\alpha)$ is a zero of f and hence $\phi(\alpha) \in K$. Therefore $\phi(K) \subset K$, $\forall \phi \in \Gamma(L : F)$. But $\phi(K) \subset K$, $\forall \phi \in \Gamma(L : F)$ implies that $\phi^{-1}(K) \subset K$, $\forall \phi \in \Gamma(L : F)$. Hence $K = \phi(\phi^{-1}(K)) \subset \phi(K)$, $\forall \phi \in \Gamma(L : F)$. Thus $\phi(K) = K$, $\forall \phi \in \Gamma(L : F)$.

Conversely, suppose that $\phi(K) = K$ $\forall \phi \in \Gamma(L : F)$ and let $g(x)$ be the minimal polynomial of α over F. Then g splits in L, since $L : F$ is a Galois extension. By proposition(1.8), F is the fixed field of $\Gamma(L : F)$. This implies that, the zeros of g are distinct, from proposition(1.5). We deduce that, g splits in K. Hence, $K : F$ is normal extension. □

(2.2) Proposition.

Let K:F be a Galois extension and let M be an intermediate field of this extension. Suppose that the extension M:F is a normal extension. Then for any F-automorphism ϕ of K, the restriction $\phi|_M$ is an F-automorphism of M.

Proof.

Let $\phi \in \Gamma(K$:$F)$ be an F-automorphism of K. Then from proposition above we have $\phi(M) = M$. Now multiply both sides by ϕ^{-1}, we get $M = \phi^{-1}(M)$. This implies that, the restrictions $\phi|_M$ and $\phi^{-1}|_M$ of ϕ and ϕ^{-1}, respectively, are both F-homomorphism mapping from M to itself. In addition, $\phi^{-1}|_M$ is the inverse of $\phi|_M$. Therefore $\phi|_M$ is an F-isomorphism and hence is an F-automorphism of M. □

Now we are ready to state and prove the main theorem of this research.

(2.3) Theorem (**Fundamental Theorem of Galois**).

Let $K : F$ be a finite Galois extension and let $G = \Gamma(K : F)$. Let

$$\mathcal{H} = \{H \subseteq G | H \text{ is a subgroup of } G\}$$

and

$$\mathcal{M} = \{M \subseteq K | M \text{ is a subfield of } K \text{ containing } F\}.$$

Then:

($\boldsymbol{i}$) $\forall M \in \mathcal{M}$, $K : M$ is a finite Galois extension.

($\boldsymbol{ii}$) There is a bijection

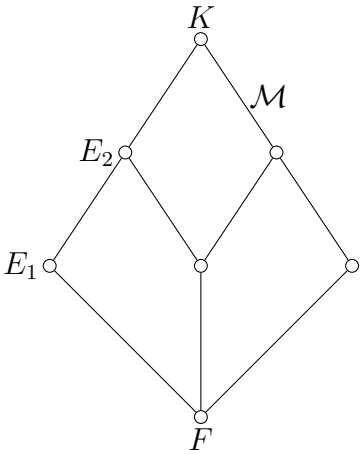
$$\phi : \mathcal{H} \longrightarrow \mathcal{M}$$

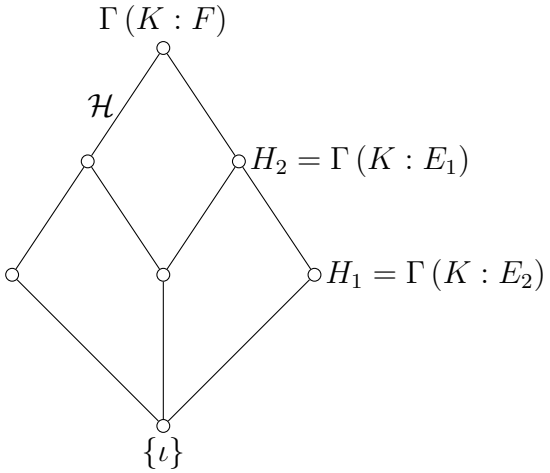
which reverses inclusion where $\forall H \in \mathcal{H}, \forall M \in \mathcal{M} : \phi(H) = F_H$ the fixed field of H and $\phi(M) = \Gamma(K : M)$.

($\boldsymbol{iii}$) $\forall M \in \mathcal{M}$:

M is normal over F if and only if the subgroup $H = \Gamma(K : M)$ is normal in G. Moreover, in this case $\Gamma(M : F) \simeq G/H$.

The following diagram show the one -to-one corresponding of (ii) above:





Proof.

($\boldsymbol{i}$) Clear from proposition(1.9).

($\boldsymbol{ii}$) Note first that $F_H \in \mathcal{M}, \forall H \in \mathcal{H}$, and by (i) $K : F_H$ is a Galois extension. Hence $\forall H \in \mathcal{H}$, $(\phi^{-1} \circ \phi)(H) = \phi^{-1}(F_H) = \Gamma(K : F_H) = H$, by proposition(1.7). Also $\forall M \in \mathcal{M}$, $(\phi^{-1} \circ \phi)(M) = \phi(\Gamma(K : M)) = M$ since $K : M$ is a Galois extension by (i). From above, we see that ϕ is a bijection. Also $\forall H_1, H_2 \in \mathcal{H}$, $H_1 \subseteq H_2$ if and only if $F_{H_2} \subseteq F_{H_1}$, i.e., $\phi(H_1) \subseteq \phi(H_2)$ if and only if $H_2 \subseteq H_1$. Thus ϕ reverses inclusion.

($\boldsymbol{iii}$) Let $H = \Gamma(K : M)$.

($\Longrightarrow$) Suppose that M is normal over F, then $M : F$ is a Galois extension by proposition(1.9). Also by proposition(2.1), $\forall \sigma \in G$,$\sigma|_M \in H$. So $\forall \tau \in H$, $\forall \sigma \in G$, we have: $\forall a \in M, (\sigma\tau\sigma^{-1})(a) = (\sigma\tau)(\sigma^{-1}(a)) = (\sigma\tau)(\sigma^{-1}|_M(a)) = \sigma(\tau(\sigma^{-1}|_M(a))) = \sigma(\sigma^{-1}|_M(a)) = \sigma(\sigma^{-1}(a)) = a$. Thus $(\sigma\tau\sigma^{-1}) \in H$, i.e., $\forall \sigma \in G, \sigma H\sigma^{-1} \subseteq H$. So H is normal subgroup of G.

($\Longleftarrow$) Assume now H is normal subgroup of G. We will show M is normal over F as follows:

Let $f(x) \in F[x]$ be an irreducible polynomial having a zero $a \in M$. Then $a \in K$ implies that $f(x)$ splits in K, since K is normal over F. Now for each zero $b \in K$ of $f(x)$, there is $\sigma \in G$ such that $b = \sigma(a)$. Since H is normal in G, $\sigma H\sigma^{-1} = H$. Hence $\forall \mu \in H, \exists \tau \in H$ such that $\mu = \sigma\tau\sigma^{-1}$. Then $\mu(b) = (\sigma\tau\sigma^{-1})(b) = (\sigma\tau\sigma^{-1})(\sigma(a)) = (\sigma\tau(a)) = \sigma(\tau(a)) = \sigma(a) = b$. Thus $b \in F_H = M$, since $K : M$ is a Galois extension. Hence all zeros of $f(x)$ are in M, i.e., $f(x)$ splits in M. Thus M is normal over F.

Finally denoting $\Gamma(M : F)$ by K and assuming H is normal in G, i.e., M is normal over F, we will show $K \simeq G/H$ as follows:

Define

$$\varphi : G \longrightarrow K$$

by $\forall \sigma \in G, \varphi(\sigma) = \sigma|_M$. Then clearly φ is well defined by proposition(2.1).

Also $\forall \sigma, \mu \in G, \forall a \in M$:$(\sigma\mu)|_M(a) = (\sigma\mu)(a) = \sigma(\mu(a)) = \sigma(\mu|_M(a)) = \sigma|_M(\mu|_M(a)) = (\sigma|_M\mu|_M(a))$. Thus $\varphi(\sigma\mu) = (\sigma\mu)|_M = (\sigma|_M)(\mu|_M) = \varphi(\sigma)\varphi(\mu)$. Thus φ is a group homomorphism. Also we have:

$\sigma \in \ker\varphi$ if and only if $\varphi(\sigma) = \iota_M$ (the identity mapping on M) if and only if $\sigma \in H$. Thus $\ker\varphi = H$ and $G/H \simeq \mathrm{Im}\varphi$. But by Tower Theorem:

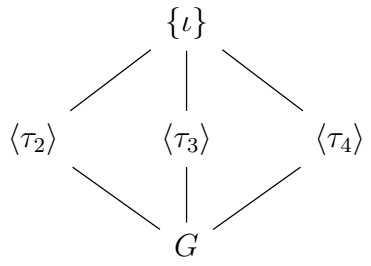
$|\mathrm{Im}\varphi| = |G|/|H| = [K : F]/[K : M] = [M : F] = |K|$. So $\mathrm{Im}\varphi = K$, since K is finite. Therefore $K \simeq G/H$ as required to show. $\square$

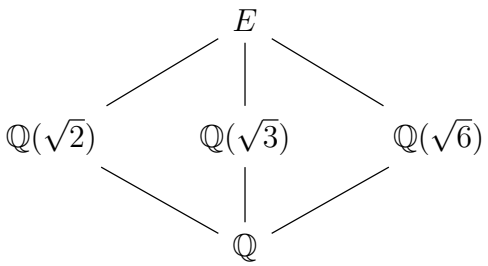
2.3 Examples of Galois Theory

(3.1) Example.

Let $h(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ and let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then clearly E is the splitting field of $h(x)$ over $\mathbb{Q}$ which means by proposition(1.3.2), E is a normal extension over $\mathbb{Q}$. Also $h(x)$ has the two irreducible factors, $x^2 - 2$ and $x^2 - 3$ and both are separable, hence $h(x)$ is separable. So $E : \mathbb{Q}$ is Galois extension. Now let $H = \Gamma(E : \mathbb{Q})$, then $|H| = [E : \mathbb{Q}] = 4$. Note that $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is a Galois extension, since $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$, so $\Gamma(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\sigma_1 = id, \sigma_2\}$ where $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Each of these mappings can be extended to $\mathbb{Q}$-automorphism of E as follows:

$\tau_1 : \sqrt{2} \longmapsto \sqrt{2}, \sqrt{3} \longmapsto \sqrt{3}, \tau_2 : \sqrt{2} :\longmapsto \sqrt{2}, \sqrt{3} \longmapsto -\sqrt{3}, \tau_3 : \sqrt{2} :\longmapsto -\sqrt{2}, \sqrt{3} \longmapsto \sqrt{3}$, and $\tau_4 : \sqrt{2} :\longmapsto -\sqrt{2}, \sqrt{3} \longmapsto -\sqrt{3}$ and each one of them has order 2 except $\tau_1 = \iota$, hence H is not cyclic which implies $H \simeq C_2 \times C_2$. By Galois corresponding, the subfields of E are $E, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}$ and the corresponding subgroups of H are $\{id_E\}, < \tau_4 >, < \tau_3 >, < \tau_2 >$, and H. Hence the inverted lattices are:





(3.2) Example.

Let $g(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then three zeros of $g(x)$ are one real root $\alpha_1 = \sqrt[3]{2}$ and two non-real roots $\alpha_2 = \omega\sqrt[3]{2}$ and $\alpha_3 = \omega^2\sqrt[3]{2}$, where ω is a cubic primitive root of unity. Clearly $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $g(x)$ over $\mathbb{Q}$ which is normal. By Eisenstein's Criterion, $g(x)$ is irreducible over $\mathbb{Q}$, hence it is separable. So $K : \mathbb{Q}$ is a Galois extension and letting $G = \Gamma(K : \mathbb{Q})$, then noting that $[K : \mathbb{Q}(\sqrt[3]{2})] = 2$ we get $|G| = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \times 3 = 6$. Now we determine the elements of G according to their permutations of zeros of $g(x)$ as follows:

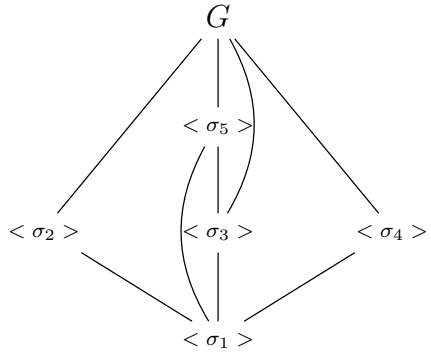
$\sigma_1 = \iota : K \longrightarrow K$, σ_2 which takes $\alpha_1 \longmapsto \alpha_2$ and fixes others,

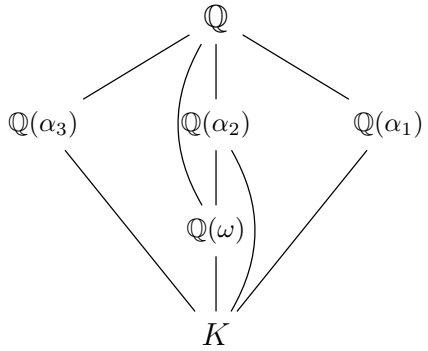
σ_3 which takes $\alpha_1 \longmapsto \alpha_3$ and fixes others,

σ_4 which takes $\alpha_2 \longmapsto \alpha_3$ and fixes others,

σ_5 which takes $\alpha_1 \longmapsto \alpha_2 \longmapsto \alpha_3$ and fixes others, and

σ_6 which takes $\alpha_1 \longmapsto \alpha_3 \longmapsto \alpha_2$ and fixes others. Now G is not abelian, since $(\sigma_4\sigma_5)(\alpha_1) = \sigma_4(\sigma_5(\alpha_1)) = \alpha_3 \neq \alpha_2 = \sigma_5(\sigma_4(\alpha_1)) = (\sigma_5\sigma_4)(\alpha_1)$. Since the only non-abelian group of order 6 is S_3, $G \simeq S_3$. The subgroups of G are $\{\sigma_1\}, <\sigma_2>, <\sigma_3>, <\sigma_4>, <\sigma_5>$, and G which correspond $K, \mathbb{Q}(\alpha_3), \mathbb{Q}(\alpha_2), \mathbb{Q}(\alpha_1), \mathbb{Q}(\omega)$ and $\mathbb{Q}$. Hence the inverted lattices are:



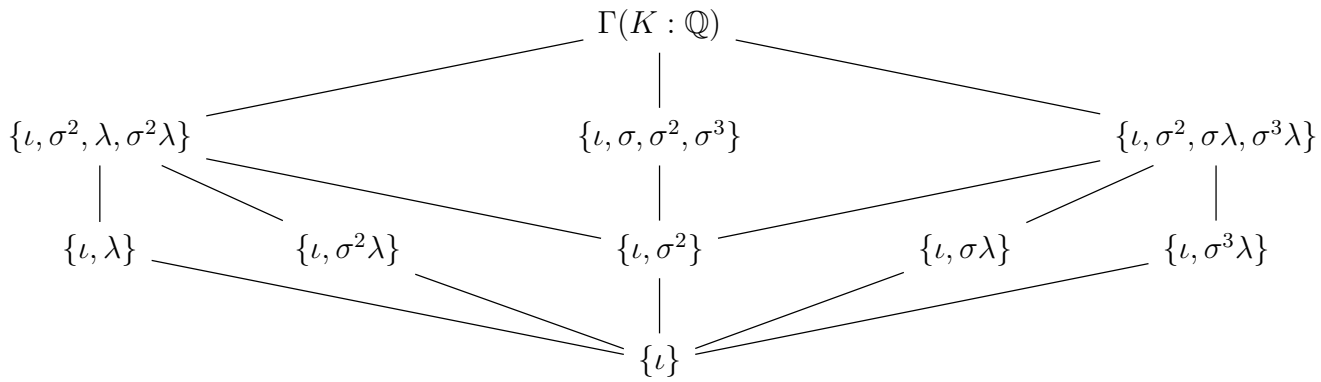


(3.3) Example.

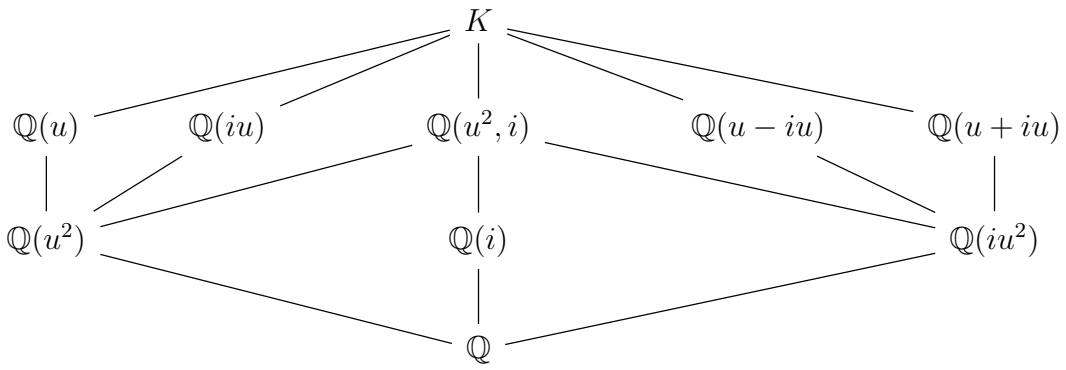
Let$f(x) = x^4 - 2 \in \mathbb{Q}[x]$ and let K be a splitting field of $f(x)$ over $\mathbb{Q}$. By Eiesenstein's Criterion, $f(x)$ is irreducible over $\mathbb{Q}$ in K and

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - u)(x + u)(x - iu)(x + iu)$$

where $u = \sqrt[4]{2}$. So the four zeros of $f(x)$ are $\pm u, \pm iu \in K$, hence $K = \mathbb{Q}(u, i)$. Now $[\mathbb{Q}(u) : \mathbb{Q}] = 4$, since $x^4 - 2$ is the minimal polynomial of u over $\mathbb{Q}$. Also $i \notin \mathbb{Q}(u)$ implies that $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(u)$ and hence $[K : \mathbb{Q}(u)] = 2$. From Tower Law, $[K : \mathbb{Q}] = [K : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 2 \times 4 = 8$. Moremore, $K : \mathbb{Q}$ is normal and separable extension by proposition(1.3.2). Hence $K : \mathbb{Q}$ is a Galois extension, so $|G| = 8 = [K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$. Thus $[K : \mathbb{Q}(i)] = 4$, so the minimal polynomial of u over $\mathbb{Q}(i)$ is of degree 4. Clearly u is a zero of the irreducible $x^4 - 2$ over $\mathbb{Q}(i)$, hence $x^4 - 2$ is the minimal polynomial of u over $\mathbb{Q}(i)$. Now proposition(1.2.3) ensures that there exists an automorphism σ of K sending u to iu which fixes i. Similarly there exits an automorphism λ of K sending i to $-i$ which fixes u. Therefore the automorphisms $\sigma, \sigma^2, \sigma^3$ and σ^4 fix i and send u to $iu, -u, -iu$ and u, respectively. Hence $\sigma^4 = \iota$ and $\lambda^2 = \iota$. Now by simple computations, we found that $\sigma^3\lambda = \lambda\sigma$, $\sigma^2\lambda = \lambda\sigma^2$, and $(\sigma\lambda)^2 = (\sigma^2\lambda)^2 = (\sigma^3\lambda)^2 = \iota$ which implies $\Gamma(K : \mathbb{Q}) = \{\iota, \sigma, \sigma^2, \sigma^3, \lambda, \sigma\lambda, \sigma^2\lambda, \sigma^3\lambda\}$. It can be shown easily that $G \simeq D_8$ the dihedral group of order 8. Finally by the Fundamental Theorem of Galois, the 10 subfields of K, namely, $K, \mathbb{Q}(u^2, i), \mathbb{Q}(u), \mathbb{Q}(u+iu), \mathbb{Q}(iu), \mathbb{Q}(u-iu), \mathbb{Q}(u^2), \mathbb{Q}(iu^2), \mathbb{Q}(i)$ and $\mathbb{Q}$ correspond to the 10 subgroups of G, namely, $\{\iota\}$, $\{\iota, \sigma^2\}$, $\{\iota, \lambda\}$, $\{\iota, \sigma\lambda\}$, $\{\iota, \sigma^2\lambda\}$, $\{\iota, \sigma^3\lambda\}$, $\{\iota, \sigma^2, \lambda, \sigma^2\lambda\}$, $\{\iota, \sigma^2, \sigma\lambda, \sigma^3\lambda\}$, $\{\iota, \sigma, \sigma^2, \sigma^3\}$ and G. Below are the two inverted lattices of this corresponding:



Supgroup of $\Gamma(K:\mathbb{Q})$



Subfields of K

2.4 Insolubility of Quintic Equations

(4.1) Definition.

Let $K : F$ be a field extension. A sequence of field extensions

$$F \subseteq F(a_1) \subseteq F(a_1, a_2) \subseteq ... \subseteq F(a_1, a_2, ..., a_n) = K$$

- where for each $i = 1, 2, ..., n$, $a_i^{n_i} \in F(a_1, a_2, ..., a_{i-1})$ for some $n_i \in \mathbb{Z}$ - is said to be a *radical sequence* and in this case K is called a *radical extension* of F.

(4.2) Example.

Let $F = \mathbb{Q}$. Then the following expression

$$\alpha = (3 + \sqrt{11})^{1/7} + \sqrt[5]{3}(\tfrac{4-\sqrt[3]{2}}{6})^{1/11}$$

is a radical expression, since it just includes nth root and basic operations: addition, multiplication, and division. Now let $a_1 = \sqrt{11}, a_2 = (3 + a_1)^{1/7}, a_3 = \sqrt[5]{3}, a_4 = \sqrt[3]{2}$ and $a_5 = (4 - a_4/6)^{1/11}$. Then $K = F(a_1, a_2, a_3, a_4, a_5)$ is a radical extension and $\alpha \in K$, since $a_1^2 = 11 \in F = \mathbb{Q}$, $a_2^7 = 3 + a_1 \in F(a_1)$, $a_3^5 = 3 \in F(a_1, a_2)$, $a_4^3 = 2 \in F(a_1, a_{2,3})$, and $a_5^{11} = (4 - a_4)/6 \in F(a_1, a_2, a_2, a_3, a_4)$.

(4.3) Definition.

Let $f(x) \in F[x]$. Then $f(x)$ is called to be *solvable by radicals* if there exists a splitting field of $f(x)$ over F which is contained in some radical extension of F.

(4.4) Definition.

A group G is said to be *solvable* if it has a finite series

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G$$

of subgroups such that for $j = 0, 1, 2, ..., n - 1$

(i) $G_j \lhd G_{j+1}$.

(ii) G_{j+1}/G_j is abelian.

From the definition above, we can clearly see that any abelian group G, G is solvable by letting $G_1 = G$ and $G_0 = \{1\}$.

(4.5) Proposition.

Suppose that G is a group, $H \leq G$, and $N \trianglelefteq G$. Then:

(i) If G is solvable, then H is solvable.

(ii) If G is solvable, then G/N is solvable.

(iii) If N and G/N are solvable, then G is solvable.

Proof.

See [1]. □

Now we proceed in investigating the relation between insolubility of a polynomial by radicals and solvability of its Galois group.

(4.6) Proposition.

Let F be a field with char(F)=0 and let K be the splitting field of $f(x) = x^n - a$, $a \in F$. Then $\Gamma(K : F)$ is solvable.

Proof.

Let u be a zero of $f(x)$ in K and let ω be a primitive nth root of unity. We have two cases:

For the case $\omega \in F$, then $u, u\omega, u\omega^2, ..., u\omega^{n-1}$ are the zeros of $f(x)$ and hence $K = F(u)$. By proposition(1.5), the elements of $\Gamma(K : F)$ send u to another zero of $f(x)$. Now we show that $\Gamma(K : F)$ is abelian and thus it is solvable as follows:
Let $\sigma, \tau \in \Gamma(K : F)$. Then $\sigma(u) = u\omega^i$ and $\tau(u) = u\omega^j$ for some i and j such that σ and τ fix ω. Therefore $(\sigma\tau)(u) = \sigma(\tau(u)) = \sigma(u\omega^j) = u\omega^i\omega^j = u\omega^{i+j}$ and $(\tau\sigma)(u) = \tau(\sigma(u)) = \tau(u\omega^i) = u\omega^j\omega^i = u\omega^{i+j}$. So $\sigma\tau = \tau\sigma$. Hence $\Gamma(K : F)$ is abelian and consequently it is solvable.

For the case $\omega \notin F$, in the equation $x^n - a$ we check two possibilities either $a = 0$ or $a \neq 0$. If $a = 0$, then $u = 0$. Therefore all elements of $\Gamma(K : F)$ fix u so $\Gamma(K : F)$ is abelian and thus $\Gamma(K : F)$ is solvable. For $a \neq 0$, then $u \neq 0$, so $u\omega/u = \omega \in K$. Hence $F(\omega) \subseteq K$, and clearly $F(\omega)$ is the splitting field of $x^n - 1$ over F. Now let $\sigma, \tau \in \Gamma(F(\omega) : F)$, then $\sigma(\omega) = \omega^i$ and $\tau(\omega) = \omega^j$ for some i and j. So $(\sigma\tau)(\omega) = \sigma(\tau(\omega)) = \sigma(\omega^j) = (\sigma(\omega))^j = (\omega^i)^j = (\omega^j)^i = (\tau(\omega))^i = \tau(\omega^i) = \tau(\sigma(\omega) = (\tau\sigma)(\omega)$. Thus $\Gamma(F(\omega) : F)$ is abelian. Now K is the splitting field of $f(x)$ over $F(\omega)$, since $F \subseteq F(\omega)$. Also $\Gamma(K : F(\omega))$ is abelian by the first case and the extension $K : F(\omega)$ is a Galois Extension. So by the Fundamental Theorem of Galois, $\Gamma(K : F(\omega)) \lhd \Gamma(K : F)$. Since we saw above that $\Gamma(K : F(\omega))$ and

$\Gamma(F(\omega) : F)$ are abelian, so they are solvable. Also by the Fundamental Theorem of Galois, $\Gamma(F(\omega) : F) \simeq \Gamma(K : F)/\Gamma(K : F(\omega))$, hence by proposition(4.5(iii)), $\Gamma(K : F)$ is solvable. □

(4.7) Proposition.

Let $f(x) \in F[x]$ with char(F)=0 and let $f(x)$ be solvable by radicals. Then $\Gamma_F(f)$ is solvable. In other words, if $\Gamma_F(f)$ is not solvable, then $f(x)$ is not solvable by radicals.

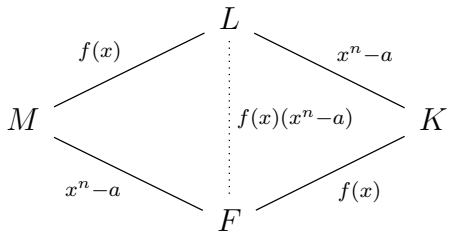
Proof.

Suppose that $f(x)$ is solvable by radicals. Then there is a radical extension $F(a_1, a_2, ..., a_s)$ which contains a splitting field K of $f(x)$ over F. So $K : F$ is a Galois extension, since it is normal over F and $f(x)$ is separable. To show that $\Gamma(K : F)$ is solvable, we proceed by induction on s.

Basic step: $s = 1$. We have $F \subseteq K \subseteq F(a_1)$, since K is the splitting field of $f(x)$ over F in $F(a_1)$. Let $a = a_1^{n_1}$ and let L be a splitting field of $g(x) \equiv x^{n_1} - a$ over F. Then $K \subseteq L$ since a_1 is a zero of $g(x)$. Since K and L are the splitting fields of $f(x)$ and $g(x)$ respectively over F, hence both are Galois extension over F. Thus by the Fundamental Theorem of Galois, we have $\Gamma(K : F) \simeq \Gamma(L : F)/\Gamma(L : K)$. By proposition above, $\Gamma(L : F)$ is solvable, and hence by proposition(4.5), both $\Gamma(L : K)$ and $\Gamma(L : F)/\Gamma(L : K)$ are solvable. Consequently $\Gamma(K : F)$ is solvable.

Induction step: Assume for $k > 1$ that the proposition holds for all $s \leq k - 1$. Now for $k = s$, let $a = a_1^{n_1} \in F$ as before, and let L be the splitting field of $g(x) \equiv x^{n_1} - a$ over K, hence by the above proposition, $\Gamma(L : K)$ is solvable. Next let $M \subseteq L$ be the splitting field of $g(x)$ over F. Since K is the splitting field of $f(x)$ over F, L is a splitting field of $f(x)g(x)$ over F. Also L is the splitting field of $f(x)$ over M, since $M \subseteq L$ is the splitting field of $g(x)$ over F. Moreover, since $F(a_1) \subseteq M$, $f(x)$ splits in $M(a_2, ..., a_s)$. So by induction hypothesis, $\Gamma(L : M)$ is solvable. Also by proposition above, $\Gamma(M : F)$ is solvable. Now by the Fundamental Theorem of Galois, $\Gamma(M : F) \simeq \Gamma(L : F)/\Gamma(L : M)$,

hence $\Gamma(L:F)/\Gamma(L:M)$ is solvable. Consequently by proposition(4.5), $\Gamma(L:F)$ is solvable which implies $\Gamma(K:F)$ is solvable, since $\Gamma(K:F) \simeq \Gamma(L:F)/\Gamma(L:K)$ by the Fundamental Theorem of Galois. $\square$



Now we need the following proposition in Group Theory.

(4.8) Proposition.

The group of permutations S_n is not solvable for all $n \geq 5$.

Proof.

See [2]. $\square$

Next we come to the last proposition needed to prove the insolubility of quintic equation.

(4.9) Proposition.

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. Suppose that $f(x)$ has exactly two non-real zeros in $\mathbb{C}$. Then $\Gamma_{\mathbb{Q}}(f)$ is isomorphic to the symmetric group S_p.

Proof.

Let $G = \Gamma_{\mathbb{Q}}(f)$. By Fundamental Theorem of Algebra, $\mathbb{C}$ must contain the splitting field K of $f(x)$, so $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_p)$ and α_i's are distinct, since $f(x)$ is separable over $\mathbb{Q}$. Now let $\sigma \in G$. Then $\sigma(\alpha_i) = \alpha_j$ for some i and j and hence the elements of G permute the zeros of $f(x)$. So G is isomorphic to a subgroup of S_p and $[K:\mathbb{Q}] = |G|$ is divisible by p, by proposition(1.7). Therefore G contains an element of order p by Cauchy's Theorem. But the elements of S_p that have order p are p-cycles which implies G has a p-cycle. Now we can restrict the complex conjugation - a $\mathbb{Q}$-automorphism of $\mathbb{C}$ - to $\mathbb{Q}$-automorphism of K that fixes $p-2$ real zeros of $f(x)$ and permutes the other two non-real zeros. Hence G has a 2-cycle. Now let G be generated by a 2-cycle $a = (12)$ and

$b = (12...p)$. Then $b^{-1}ab = (23) \in G, b^{-1}(23)b = (34) \in G, b^{-1}ab = (45) \in G$ and so on. Hence G contains all the transpositions of the form $(n, n+1)$. Also $a^{-1}(23)a = (13) \in G, (13)(34)(13) = (14) \in G$ and so on. Therefore G contains all the transpositions of the form $(1n)$. Moreover, $(1n)(1m)(1n) = (nm) \in G$. But we know that every element in S_p is the product of transpositions.It follows that, $G = S_p$. $\square$

Finally we state and prove the most important conclusion of this research, i.e., the insolubility of the quintic equation.

(4.10) Theorem.

Let $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Then $f(x)$ is not solvable by radicals. So no general law for solving quintic equations by radicals.

Proof.

First we show that $f(x)$ has exactly three real roots and two non-real roots as follows: $f(-2) = -17$ and $f(-1) = 8$, so there is a real root on [-2,-1]. Also $f(0) = 3$ and $f(1) = -2$ means there is another real root on [0,1]. Moreover, $f(2) = 23$ implies there is a third real root on [1,2]. Now $f'(x) = 5x^4 - 6$ has the two real roots $\pm\sqrt[4]{6/5}$. Hence by Rolle's Theorem, $f(x)$ has at most three real roots which we have already found.Thus $f(x)$ has exactly three real zeros and two non-real zeros. Also $f(x)$ is irreducible over $\mathbb{Q}$, by Eisenstein's Criterion. So by the above proposition, $\Gamma_{\mathbb{Q}}(f) \simeq S_5$, hence is not solvable. Thus by proposition(4.7), $f(x)$ is not solvable by radicals. $\square$

References

1. J.Gallian; Contemporary Abstract Algebra; Seventh edition; Brooks/COLE; 2010.

2. J.Howie; Fields and Galois Theory; Springer; 2006.

3. P.McCarthy; Algebraic Extensions of Fields; Dover Publications, Inc, 1991.

4. I. Stewart; Galois Theory; Third edition; Chapman & Hall/cRc; 2004.

5. D.Wilkins; Lecute Notes on Galois Theory; Web PDF file 2007.