Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématique Discrète

Thème

Galois Extension and its apllications

Présentée par :
M^r Harzelli Mohamed Rafik

Devant le jury composé de :

Dechoucha Noureddine	MAA.	Université de M'sila	**Président**.
Ladjelat Lahcene	MAA.	Université de M'sila	**Encadreur**.
Khadraoui Abdelmalek	MAA.	Université de M'sila	**Examinateur**.
Berrabah Imzdeddine	E.Doctorant	Université de M'sila	**Invité** .

Année universitaire 2021/2022.

.

Contents

Introduction

Throughout the history of mathematics, the problem of solving algebraic equations has been important problem. the Babylonians,Egyptian,Chinese and Hinder civilizations dealt with the solution of equations of the first and second degree. The geometric viewpoint of the Greeks,reflects,according to the Greeks, the true geometrical state of the universe. They solved quadratic equations by " completing the square ". there were no negative root because it did not have any geometrical significance.

Moslems gave the name " algebra " to the current known branch of mathematics. the quadratic formula for equations of degree two, which is one of beautiful significant algebraic results, date from the Moslem era.

From then on until the eighteenth century the solution of algebraic equation by radicals, i.e, expressions involving roots and arithmetic operations, was a natural problem to consider.

Abel showed that the solution by radicals of general equation of fifth degree is impossible. E. Galois gave the complete answer that the general equation of degree n is not solvable by radicals if $n \geq 5$.

The purpose of this work is to provide an introduction to Galois extension of a field and some of its applications : the solvability of equations by radicals. To achieve this ourpose the work is divided into three chapters :

• In the first chapter contains summaries of the necessary requirements from : field theory.notions of extensions, algebraic and transcendental elements. the core of this chapter consists of on paragraph 1.5 and 1.6 : the normal and separable extension.

• In the second chapter, we begin to study the theory of Galois extensions and some of its properties with the notion of Galois group together. In order to state the Fundamental theory of correspondence of Galois.

• In the last chapter we give an applications of the theory ton the famous problem of solving algebraic equation by radicals using the notion of solvable groups.

Chapter 1

Field extensions

1.1 Field extensions

1.1.1 Some preliminaries on extensions

Definition 1.1.1 *Let's assume F and E are two fields . If F is a subfield of E, E is an extension field of F (or simply E is an extension of F). E/F denotes a field extension.*

Example 1.1.1 *(1) $\mathbb{R}$ is an extension of $\mathbb{Q}$.*
(2) $\mathbb{C}$ is an extension of $\mathbb{R}$.

Remark 1.1.1 *Let's call the field extensions E/K and L/K. A K-homomorphism is a homomorphism $\phi : E \to L$ that has $\phi(a) = a$ for all $a \in K$. It's written a K-isomorphism when 'ϕ is also an isomorphism. We say that E and L are K-isomorphic.*

Remark 1.1.2 *E is a vector space of F with the intern operation if E is an extension of F.*

$$+ : E \times E \to E$$
$$(x, y) \longrightarrow x + y$$

and the product by a Scalar product (extern operation)

$$. : F \times E \longrightarrow E$$
$$(\lambda, x) \longrightarrow \lambda.x$$

Proposition 1.1.1 *let E be an extension of F and let $\alpha \in E$, we define:*

$$F[\alpha] = \{f(\alpha)\,|f(x) \in F[x]\}$$

and

$$F(\alpha) = \{f(\alpha)/g(\alpha)|f(x), g(x) \in F[x] \text{ with } g(\alpha) \neq 0\}$$

So:

1. *The smallest subring of E that contains both $alpha$ and F is $F[\alpha]$.*
2. *The smallest subfield of E containing $alpha$ and F is $F(\alpha)$.*

Proposition 1.1.2 *Let F be a field, E be its extension, and S be its subset. If $S = S_1 \cup S_2$, then*

$$F(S) = F(S_1)(S_2)$$

Proof.
We have $F(S_1)(S_2)$ is a subfield of E containing $F(S_1)$ and S_2 so $F(S_1)(S_2) \supset F, S_1, S_2$ hence $F(S_1)(S_2) \supset F(S)$....(1)
we have $S_1 \subset S$ so $F(S_1) \subset F(S)$ and the other hand $S_2 \subset F(S)$
so $F(S_1)(S_2) \subset F(S)$....(2)
from (1) and (2) we have

$$F(S) = F(S_1)(S_2)$$

■

Definition 1.1.2 *The dimension of E as a F-vector space is the degree of the field extension E/F (with $[E : F] = \infty$ if this is not a finite dimensional vector space). If $[E : F] < \infty$, the field extension E/F is considered finite.*

Remark 1.1.3 $[E : F]$ = *1 if and only if $E = F$.*

Proof.
$[E : F] = 1$*if and only if 1 is a F-basis of E if and only if $E = F.1 = F$* ■.

Definition 1.1.3 *Consider the field extension E/F. An intermediate field of E/F is defined as a subfield $L \subset E$ with $F \subset L$.*

Theorem 1.1.1 *(Degree theorem) Let L be an intermediate field of a field extension : E/F so*

$$[E : F] = [E : L][L : F]$$

Proof.

If E/L or L/F isn't finite, E/F isn't finite either. Assume that the extensions E/L and L/F are finite field extensions. Let $(x_1, \ldots, x_n)$ be a L over F basis and $(y_1, \ldots, y_m)$ be a E over L basis. We will proof $A = \{x_i y_j \mid x_i \in L\ y_j \in E\}$. A basis of E over F for $1, \ldots, n, j = 1, \ldots, m$. They engender: We can write $y \in E$ if $y \in E$.

$$y = \sum_{j=1}^{m} b_j y_j, \quad b_j \in L,$$

and for all j we have:

$$b_j = \sum_{i=1}^{n} a_{ij} x_i, \quad a_{ij} \in F.$$

Thus we get $y = \sum_{i,j} a_{ij} x_i y_j$. They are linearly independent: If

$$\sum_{i,j} a_{ij} x_i y_j = 0, \quad a_{ij} \in F,$$

Then for all j, we obtain $\sum_{i=1}^{n} a_{ij} x_i = 0$ because the y_j are linearly independent over L, and therefore for all i, j, we get $a_{ij} = 0$ since the x_i are linearly independent over F, hence A is a basis of E over F. ■

Corollary 1.1.1 *$[L : F]$ divides $[E : F]$ if L is an intermediate field of a finite field extension $[E : F]$. The only intermediate fields are F and F, especially if $[E : F]$ is a prime number.*

1.2 Simple extensions and Algebraic extensions

Definition 1.2.1 *A field extension E/F is called a simple extension if there exists an element $\alpha \in E$ with $E = F(\alpha)$.*

Example 1.2.1 *1) $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\right\}$ is a simple extension of $\mathbb{Q}$.*
2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} | a, b, c, d \in \mathbb{Q}\right\}$ is a simple extension of $\mathbb{Q}(\sqrt{2})$.

Definition 1.2.2 *Let E/F be a field extension, and $\alpha \in E$ be an element. If there is a nonzero polynomial $f \in F[X]$ such that $f(\alpha) = 0$, we say α is algebraic over F. We say α is transcendental over F if it is not algebraic over F. If all elements of E are algebraic over F, it is termed an algebraic extension of F.*

Example 1.2.2 *$\alpha \in F \Rightarrow \alpha$ is algebraic over F. For α is a zero of $(X - \alpha) \in F[X]$.*

Example 1.2.3 *Let $F = \mathbb{Q}, E = \mathbb{C}$. Then $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt[3]{7}, \alpha_3 = \sqrt{2} + \sqrt[3]{7}$ are all algebraic over* **Q**. *For α_1 is a zero of $X^2 - 2$; α_2 is a zero of $X^3 - 7$; α_3 is a zero of $X^6 - 6X^4 - 14X^3 - 12X^2 - 84X + 41$.*
$\pi = 3.1415926$, $e = 2.718281$ are transcendental over $\mathbb{Q}$,

Theorem 1.2.1 *(Gelfond-Schneider) : Let $\alpha \neq 0, 1$ be algebraic over $\mathbb{Q}$. Let β be algebraic over $\mathbb{Q}, \beta \notin \mathbb{Q}$. Then α^β is transcendental over $\mathbb{Q}$.*

Example 1.2.4 *$2^{\sqrt{2}}$ is transcendental over $\mathbb{Q}$.*

Theorem 1.2.2 *If E is a finite field extension on F and $\alpha \in E$ is an algebraic over F, then $f_\alpha(X) \in F[X]$ is a unique normalizes polynomial (leading coefficient equal 1) such that:*

1. *$f_\alpha(\alpha) = 0$.*
2. *f_α is irreducible.*
3. *if $g(x) \in F[X]$ such that $g(\alpha) = 0$ then. $f_\alpha(X)$ divide $g(X)$.*

Remark 1.2.1 *we denote the polynomial $f_\alpha(X) \in F[X]$ The minimal polynomial f_α of α over F we write $f_\alpha(x) = Irr(\alpha, F, X)$.*

Example 1.2.5 *By the Eisenstein criteria, we know that $x^n - p$ is irreducible in $\mathbb{Q}[x]$ for each prime integer p and all $n \in \mathbb{N}$. As a result, $x^n - p$ is the minimal polynomial for $\sqrt[n]{q}$ over $\sqrt[n]{q}$.*

Definition 1.2.3 *By definition, the degree of α on F equals the degree of $f_\alpha(X)$ (f_α is the minimal polynomial) we write*

$$deg(F(\alpha)) = deg(f_\alpha(X))$$

Theorem 1.2.3 *Let α be algebraic over $F, n = \deg(\mathrm{Irr}_F(\alpha, X))$. Then*
(1) $F(\alpha) \simeq F[X]/(f_\alpha(X))$
(2) $\deg(F(\alpha)/F) = deg(f_\alpha(X)) = n$.
(3) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ *is a basis for $F(\alpha)$ over F.*

Remark 1.2.2 *Let $F(b)/F$ is a simple algebraic extension of degree n and the minimal polynomial of b over F be $f = \sum_{i=0}^{n} a_i X^i$ Then, according to the Theorem, $F(b)$ may be expressed directly as follows:*

$$F(b) = \left\{ \sum_{i=0}^{n-1} c_i b^i \mid c_i \in F \right\}.$$

The conventional ones are addition and multiplication, as though these were polynomials in the indeterminate b, with the condition that we delete any power of two. b bigger than $n-1$ by $b^n = -\sum_{i=0}^{n-1} a_i b^i$.

Example 1.2.6 *. The minimal polynomial of i over $\mathbb{R}$ is x^2+1. Thus $\mathbb{C} = \mathbb{R}[X]/(X^2+1) = \mathbb{R}(i) = \{a+bi \mid a,b \in \mathbb{R}\}$, with addition and multiplication*

$$(a+bi)+(c+di) = a+c+(b+d)i$$

$$(a+bi)(c+di) = ac+(ad+bc)i+bdi^2 = ac-bd+(ad+bc)i$$

Theorem 1.2.4 *Consider the field extension E/F ,E/F is a finite extension if and only if E/F is algebraic and there are finitely many elements $a_1, a_2, .., a_n \in E$ such that $E = F(a_1, a_2, ..., a_n)$.*

Proof.

Let $n = [E:F]$. Then for any $a \in E$ the elements $1, a, \ldots, a^n$ are linearly dependent. Thus there exists a nonzero polynomial $f \in F[x]$ with $f(a) = 0$. If $a_1, \ldots, a_n$ is a basis of E over F, then $E = F(a_1, \ldots, a_n)$.

Conversely We will prove this by induction on n, the case $n = 0$ being trivial. Assume that $E = F(a_1, \ldots, a_{n+1})$ and that for $L = F(a_1, \ldots, a_n)$ the degree $n = [L:F]$ is finite. Let g be the minimal polynomial of a_{n+1} over L. Then $[E:L] = \deg(f)$ and $[E:F] = [E:L][L:F] = \deg(f).n$ is finite.

This result implies that the elements of F which are algebraic over F form an intermediate field of E/F. ■

Corollary 1.2.1 *Let $L = \{a \in E \mid a$ is algebraic over $F\}$. Then L is an algebraic extension of E/F and L/F is a subfield of E/F.*

Proof.

Let $a, b \in L$ then a, b is algebraic over F with $T = F(a,b)$, T is finite extension of F we know $T \subset L$ then $a-b, a/b \in T$ So L is field and by definition L/F is an algebraic extension. ■

Example 1.2.7 *we have $\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid a$ is algebraic over $\mathbb{Q}$ we called it is the field of algebraic numbers. It is an (infinite) algebraic extension of $\mathbb{Q}$.*

Corollary 1.2.2 *Let's call the algebraic field extensions E/L and L/F. so E/F is also algebraic field extension.*

1.3 Algebraic closure

Definition 1.3.1 *If every nonconstant $f \in F[X]$ has a root in F, the field is said to be algebraically closed.*

Definition 1.3.2 *Every nonconstant polynomial in $F[X]$ splits into a product of linear factors over F thus we say that field F is said to be algebraically closed.*

$$f(X) = b.\prod_{i=1}^{n}(X - a_i) \quad a_i \in F$$

Remark 1.3.1 *the two previous definitions are equivalent*

Example 1.3.1 *1) $\mathbb{C}$ is algebraically closed By Gauss's theorem.*

2) $\mathbb{Q}$ is not algebraically closed because $x^2 - 3$ has no zero in $\mathbb{Q}$.

3) $\mathbb{R}$ is not algebraically closed, because $x^2 + x + 1$ has no zero in $\mathbb{R}$.

4) $\overline{\mathbb{Q}}$ is algebraically closed.

Proposition 1.3.1 *The following statements are equivalent:*

(1) F is algebraically closed.

(2) If E is an algebraic extension of F, hence $E = F$.

Theorem 1.3.1 *Assume F is a field. Then an algebraically closed extension E of F exists.*

Definition 1.3.3 *An algebraic closure of a field F is an extension $\bar{F}$ of F such that*

(1) $\bar{F}$ is algebraically closed,

(2) $\bar{F}$ is an algebraic extension of F.

Theorem 1.3.2 *Let F be a field. Then F has an algebraic closure.*

1.4 Splitting fields

Theorem 1.4.1 *There is a E extension of F that contains a f zero.*

Proof.

If f_1 is an irreducible factor of f in $F[X]$, then every zero of f_1 is also a zero of f. Therefore, without loss of generality,assume that f is irreducible in $F[X]$ and $F[X]$ is is a PID (Principal ideal Domain) then $I = (f)$ is a maximal ideal, Thus $E = F[X]/(f)$ is a field , we define the map $\phi : F \longrightarrow K$ with $\phi(a) = a + I$ so we have $F \cong E$, let us identify F with the subring $\{a + I | a \in F\}$ of E, so that we can view E as an extension of F.

We proof that f has a zero in E,denote the class $[x]$: Write $f = \sum_{i=0}^{n} a_i x^i$ with $a_i \in F$. Then

$$0 = [f] = \sum_{i=0}^{n} [a_i] \left[x^i\right] = \sum_{i=0}^{n} a_i [x]^i = f([x]).$$

Thus $[x]$ is a zero of f in K, and $E = F([x])$. ■

Remark 1.4.1 *we say that E is obtained from F by formally adjoining a root of f.*

Corollary 1.4.1 *Let $f \in F[x]$ be a polynomial of degree $n > 0$. Then there exists Then there's a field extension E/F with $[E : F] \leq n$ and f has a zero in E.*

Definition 1.4.1 *Let $f \in F[x]$ by a polynomial of degree $n > 0$. A splitting field of f over F is a finite extension E/F if:*

(1) f splits over E into linear factors, i.e. there exist $a_1, \ldots, a_n, b \in K$ such that $f = b\,(x - a_1) \cdot \ldots \cdot (x - a_n)$.

(2) f does not split over any intermediate field $E \supsetneq L \supset F$.

Corollary 1.4.2 *Let $f \in F[x]$ be monic with deg$(f) = n$,$n > 0$.*

(1) If L/F is an extension of F with f splits into linear factors $x - a_1, \ldots, x - a_n$ then $F(a_1, \ldots, a_n)$ is a splitting field of f over F.

(2) There exists a splitting field K of f over F with $[K : F] \leq n!$.

(3) Let K be a splitting field of f over F, and L be an intermediate field. Then K is a f splitting field over L as well.

Proof.

(1) Let L/F be a field extension such that we have $f = (x - a_1) \ldots (x - a_n)$ with $a_i \in L$. we proof that $L = F(a_1, \ldots, a_n)$ is a splitting field of f over F, we have f splits into linear factor over F, assume that $K \subset F$ such that f splits into linear factors, $f = (x - c_1) \ldots (x - c_n)$ $c_i \in K$. for all i we have $f(a_i) = 0$ so $0 = f(a_i) = (a_i - c_1) \ldots (a_i - c_n)$. hence $a_i = c_j$ for some j thus

$a_i \in K$ *Therefore* $F = K$.

(2) by the previous corollary (1.4.1) there is a field extension K_1/F *with* $[K_1 : F] \leq n$ *such that* f *has a zero* $a_1 \in K_1$*, then* $f = (x - a_1)\, g$ $\deg(g) \leq n - 1$ $g \in K_1[X]$ *and by induction there is a finite field extension* K/K_1 *of degree* $\leq (n-1)!$ *such that* g *splits over* K *into linear factors with* $[K : K_1] \leq (n-1)!$ *so by the degree theorem we have* $[K : F] = [K : K_1][K_1 : F] \leq n!$ *such that* f *splits over* K *into linear factors.*

(3) We have $f \in F[X]$ *so* $f \in L[X]$ *and* f *splits over* L *and there is no intermediate field between* L *and* K *where it splits.* ■

Example 1.4.1 *(1)* $\mathbb{C}$ *is a splitting field of* $x^2 + x + 1$ *over* $\mathbb{C}$ *and* $\mathbb{Q}[\sqrt{3}]$ *is a splitting field of* $x^2 - 3$ *over* $\mathbb{Q}$*.*

(2) More generally let $f \in F[x]$ *be an irreducible polynomial of degree* 2 *with a zero in* K *and* K/F *is an extension of degree 2 such that* f *having a zero in* K*. Then* K *is a splitting field of* f *over* F*.*

(3) (Splitting field of $x^4 + 1$ *over* $\mathbb{Q}$ *). Let* $\alpha \in \mathbb{C}$ *be a root of* $x^4 + 1$ *in an extension of* $\mathbb{Q}$*. Then also* $-\alpha, \frac{1}{\alpha}$ *and* $-\frac{1}{\alpha}$ *are roots of* $x^4 + 1$*. These roots are distinct:* $\alpha \neq -\alpha$ *because* $\alpha \neq 0$ *and if* $\alpha = \pm\frac{1}{\alpha}$*, then* $\alpha^2 = \pm 1$*; thus* $\alpha^4 + 1 = 2 \neq 0$*. Thus over* $\mathbb{Q}(\alpha)$ *we get*

$$x^4 - 1 = (x - \alpha)(x + \alpha)\left(x - \frac{1}{\alpha}\right)\left(x + \frac{1}{\alpha}\right).$$

Therefore $\mathbb{Q}(\alpha)$ *is the splitting field of* $x^4 + 1$*.*

(4) (Splitting field of $x^3 - 3$ *). Over the complex numbers we have with* $\omega = e^{2\pi i/3}$

$$x^3 - 3 = (x - \sqrt[3]{3})\left(x - \omega\sqrt[3]{3}\right)\left(x - \omega^2\sqrt[3]{3}\right).$$

Clearly $x^3 - 3$ *splits over* $\mathbb{Q}\left(\sqrt[3]{3}, e^{2\pi i/3}\right)$*, but it does not split over* $\mathbb{Q}(\sqrt[3]{3})$ *or* $\mathbb{Q}\left(e^{2\pi i/3}\right)$*, because* $\sqrt[3]{3}$ *is real and* $\mathbb{Q}\left(e^{2\pi i/3}\right)$ *does not contain* $\sqrt[3]{3}$*.*$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ *and* $\left[\mathbb{Q}\left(e^{2\pi i/3}\right) : \mathbb{Q}\right] = 2$*. Thus* $\left[\mathbb{Q}\left(\sqrt[3]{3}, e^{2\pi i/3}\right) : \mathbb{Q}\right] = 6$*.*

1.4.1 Extension of field isomorphism to splitting fields

Definition 1.4.2 *Let* $\varphi : K \to K'$ *a field isomorphism and let* $F/K, F'/k'$ *be field extensions. An isomorphism* $\Phi : F \to F'$ *is called an extend (extension) of* φ*, if* $\Phi|_K = \varphi$*.*

Definition 1.4.3 *An isomorphism of fields is $\varphi : K \to K'$ hen an isomorphism is defined by*

$$\varphi_* : K[x] \to K'[x]; f = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i) x^i$$

Theorem 1.4.2 *Let $\varphi : k \to k'$ be a field isomorphism. Let L/K and L'/K' be field extensions. Let $a \in L$ be algebraic over K with minimal polynomial f_a. Let $a' \in L'$ be a zero of $\varphi_*(f_a)$. Then there is a unique extension $\Phi : K(a) \to K'(a')$ of φ with $\Phi(a) = a'$.*

Corollary 1.4.3 *Let F/k be a field extension and let $a, a' \in F$ be algebraic with the same minimal polynomial. Then there exists a unique k-isomorphism $\varphi : k(a) \to k(a')$ with $\varphi(a) = a'$.*

Theorem 1.4.3 *Let $\varphi : K \to K'$ be an isomorphism of fields. Let $f \in K[x]$ be a nonzero polynomial and $\widehat{f} = \varphi_*(f)$. Let F be the splitting field of f over K and F' the splitting field of $\widehat{f}$ over K'. Then there is an isomorphism $\Phi : F \to F'$ with $\Phi|_K = \varphi$. In particular if F, F' are splitting fields of f over K then there is a K-isomorphism $\Phi : F \to F'$.*

Proof.

By induction ,if $[F : K] = 1$ then $F = K$ thus f splits into linear factor over K then $\widehat{f}$ splits into linear factor over F' (because φ is an isomorphism) so $K' = F'$ and $\Phi = \varphi$.

if $[F : K] > 1$ then f has an irreducible factor $g \in K[X]$ with $deg(g) > 2$ thus $\widehat{g} = \varphi_*(g)$ is an irreducible factor of $\widehat{f}$ with $deg(g) = deg(\widehat{g})$,let a be a zero of g in F and a' zero of $\widehat{g}$ in F' so by the previous theorem there exist an isomorphism $\varphi' : K(a) \to K'(a')$ with $\varphi'(a) = a'$ and clearly $[F : K(a)] < [F : K]$ so F splitting field of f over $K(a)$ and F' is splitting field of $\widehat{f}$ over $K'(a')$ so by induction there is an isomorphism $\Phi : F \to F'$. with $\Phi|_{K(a)} = \varphi'$.thus $\Phi|_K = \varphi$.

such that we have Commutative diagram:

$$\begin{array}{ccc}
\varphi : K & \xrightarrow{\varphi} & K' \\
\downarrow & & \downarrow \\
\varphi' : K(a) & \xrightarrow{\varphi'} & K'(a') \\
\downarrow & & \downarrow \\
\Phi : F & \xrightarrow{\Phi} & F'
\end{array}$$

■

1.5 Normal extensions

Definition 1.5.1 *A field extension E/F is called normal if it is algebraic and every irreducible polynomial $f \in F[X]$ has a zero in E splits over E.*

Example 1.5.1 *(1) $\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)/\mathbb{Q}$ is a normal extension.*
(2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a normal extension.
(3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal because $X^3 - 2$ has a zero in $\mathbb{Q}(\sqrt[3]{2})$ but does not splits into linear factor over $\mathbb{Q}(\sqrt[3]{2})$.

Proposition 1.5.1 *A finite extension E/k is a normal if and only if E is splitting field over k with a polynomial in $k[x]$.*

Proof.

Let E/k be finite extension thus $E = k(a_1, a_2, ..., a_n)$ and let g_i be a minimal polynomial of a_i such that $g_i \in k[x]$ so we put $g = g_1.g_2...g_n$ since E/k a normal extension then g_i splits over E into linear factors thus g splits into linear factors , so $E = k(a_1, a_2, ..., a_n)$ is splitting field of g over k.

Conversely, Let E be a splitting field of f over k ,let be $g \in k[x]$ be irreducible polynomial and Let $\alpha \in E$ zero of g we will show g splits into linear factors over k let β be a zero of g we show that $\beta \in E$ in the same way to show the other zeros of g belongs to E (it follows by induction) ,since be irreducible then there is an k-isomorphism $\varphi : k(\alpha) \to k(\beta)$ we have E is splitting field of f over $k(\alpha)$ and $E(\beta)$ splitting field over $k(\beta)$ of f then there exist an isomorphism $\phi : E \to E(\beta)$ such that $\phi|_{k(\alpha)} = \varphi$ and $\phi|_k = id_k$ thus we have isomorphism k-vector spaces so $[E : k] = [E(\beta) : k]$ and by the degree theorem we get $[E(\beta) : E] = 1$ thus $E = E(\beta)$ and $\beta \in E$. ■

1.6 Separable extensions

Definition 1.6.1 *Let F be a field and let $f(x) \in F[x]$ be a polynomial. Over a splitting field for $f(x)$ we have the factorization.*

$$f(x) = (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct elements of the splitting field and $n_i \geq 1$ for all i. Remember that if α_i is called a multiple root if $n_i > 1$ and is called a simple root if $n_i = 1$. The integer n_i is called the multiplicity of the root α_i.

Definition 1.6.2 *If a polynomial f over F has no multiple roots (i.e., all of its roots are distinct), it is said to be separable. Inseparable polynomials are those that cannot be separated.*

Definition 1.6.3 *An algebraic field extension F/k is called separable if all irreducible polynomials $f \in k[x]$ with a zero in F have only simple roots in their splitting fields. Equivalently the minimal polynomial of any $a \in F$ has only simple roots in its splitting field. If every algebraic extension F/k is separable over k, then k is called perfect.*

Example 1.6.1 *The polynomial $x^2 - 3$ is separable over $\mathbb{Q}$ since its two roots $\pm\sqrt{3}$ are simple. The polynomial $(x^2 - 2)^n$ for any $n \geq 2$ is inseparable since it has the multiple roots $\pm\sqrt{2}$, each with multiplicity n.*

Definition 1.6.4 *Let $f = \sum_{i=0}^{n} a_i x^i \in k[x]$. The derivative of f is $f' := \sum_{i=1}^{n} i a_i x^{i-1}$.*

Lemma 1.6.1 *Let $f \in k[x]$ be a nonconstant polynomial and let E/k be a splitting field of f, let $a \in E$ be a zero of f. Then a is a multiple root of f if and only if $f'(a) = 0$.*

Proof.

Let $a \in E$ be a multiple root of f then $f(x) = (x-a)^m.g(x)$ such that $g(a) \neq 0$ so $f'(x) = m.(x-a)^{m-1}.g(x) + (x-a)^m.g'(x)$ so $f'(a) = 0$ then $f(a) = f'(a) = 0 \iff m > 1$ ■

Theorem 1.6.1 *Consider the irreducible polynomial $f \in F[x]$, f has no multiple roots in its splitting field over F . If and only if $f' \neq 0$.*

Proof.

The inverse implication, Let E/F be a splitting field of f over F,If $f' = 0$ then all roots of f are multiple.

Conversely, Let $a \in E$ be a multiple roots of f we have f irreducible polynomial so f is minimal polynomial of a over F (by multiplying of a constant in f) we have $f(a) = f'(a) = 0$ so $f|f'$ and we have $deg(f') < deg(f)$ if $f' \neq 0$.$f' \neq 0$so we get a contradiction. ■

Proposition 1.6.1 *f is separable if and only if f is relatively prime to its derivative.*

Corollary 1.6.1 *Every irreducible polynomial with characteristic 0 (for example $\mathbb{Q}$) may be separated.*

Proof.

Let F be a field with Char(F)=0 $f(x) = \sum_{i=0}^{n} a_i x^i$. so $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$ with $f \in F[X]$ if $f'(x) = 0$ then $i.a_i = 0$ for all $i \in \{1, 2..., n\}$ since Char(F)=0 so $a_i = 0$ for all $i \in \{1, 2..., n\}$ so $f(x) = a_0$ thus we get a contradiction because f is irreducible with deg$(f) \geq 1$ so $f'(x) = 0$ and by the previous theorem (1.6.1) f is separable. ■

Corollary 1.6.2 *Every field of characteristic 0 is perfect.*

Proof. *In a field of characteristic zero, the derivative of a nonconstant polynomial isn't zero. So we take an extension algebraic E/F by the minimal polynomial $f \in F[x]$ with Char(F)=0 so we get a separable extension because the minimal polynomial all its roots are simple.* ■

Theorem 1.6.2 *(Theorem of the primitive element) Let F be a finite separable field extension of k Then there exists an element $a \in F$ with $F = k(a)$.*

Chapter 2

Galois Theory

2.1 Galois groups

Definition 2.1.1 *Let E/F be a field extension. Let Aut(E/F) be the set of E automorphisms when F is fixed.*

Definition 2.1.2 *Let E/F be a field extension An F-isomorphism of E onto itself is an F-automorphism of E.The Galois group is a set of all all F-automorphisms of E denoted Gal(E/F): such that:*

$$Gal(E/F) = \{\, \varphi \in Aut(E) \;\mid\; \varphi(a) = a \;,\; for \;\; all \;\; a \in F\}$$

Example 2.1.1 *Gal($\mathbb{C}/\mathbb{R}$)=$\{id, \tau\}$ such that $\tau : \mathbb{C} \to \mathbb{C}$, $a + bi \to a - bi$.*

Notation 2.1.1 *For a finite set M we define $S(M)$ by $S(M) := \{\sigma : M \to M$ bijection $\}$ such that $S(M)$ is the set of all permutations of M ,If $n = |M|$ then $S(M) \cong S_n$.*
Remember that an action of a group G on M is simply transitive if for all $h_1; h_2 \in M$ there is a unique $g \in G$ with $g(h_1) = h_2$. Then Clearly $|M| = |G|$ (just fixing one element of M).

Theorem 2.1.1 *Let $F(a)/F$ be a simple algebraic extension of degree n,let f be a minimal polynomial of a over f we define $\mathcal{R} = \{\alpha \in F(a) \mid f(\alpha) = 0\}$ the set of zeros of f thus Gal($F(a)/F$) acts simply transitively on $\mathcal{R}$ and Gal($F(a)/F$) isomorphic to a subgroup of $S(\mathcal{R})$ of order $|\mathcal{R}|$.*
Proof.
Let $\varphi \in Gal(F(a)/F)$ and $g \in F[X]$ with $g = \sum_{i=0}^{n} a_i x^i$ if $b \in \mathcal{R}$ we get :

$$\varphi(g(b)) = \sum_{i=0}^{n} a_i \varphi(b)^i = g(\varphi(b))$$

so

$$\varphi(f(b)) = f(\varphi(b)) = 0$$

thus $\varphi(b)$ is zero of f then $\varphi(b) \in \mathcal{R}$ so we get $\varphi|_{\mathcal{R}}$ maps into itself since φ is is injective so $\varphi|_{\mathcal{R}}$ is injective As $\mathcal{R}$ is finite set so $\varphi|_{\mathcal{R}}$ is is a bijection thus $\varphi|_{\mathcal{R}} \in S(\mathcal{R})$, we define a map

$$\Phi : \mathit{Gal}(F(a)/F) \twoheadrightarrow S(\mathcal{R})$$

with $\varphi \to \varphi|_{\mathcal{R}}$ we are clearly $\Phi$is a group homomorphism i.e :$(\varphi \circ \psi)\,|_{\mathcal{R}} = \varphi|_{\mathcal{R}} \circ \psi|_{\mathcal{R}}$, we take $r_1, r_2 \in \mathcal{R}$ then by ***the corollary*** *(1.4.3) there exist a unique $\varphi \in \mathit{Gal}(F(a)/F)$ with $\varphi(r_1) = r_2$ so $\mathit{Gal}(F(a)/F)$ acts simply transitivity on $\mathcal{R}$ and we have Φ is injective (because ker(Φ)=$id|_{F(a)}$ since $\mathit{Gal}(F(a)/F)$ acts simply transitivity on $\mathcal{R}$ thus we take any $r \in \mathcal{R}$ the exist a unique $\varphi \in \mathit{Gal}(F(a)/F)$ s.t $\varphi(r) = r$ so $\varphi = id|_{F(a)}$) then $\mathit{Gal}(F(a)/F)$ isomorphic to a subgroup of $S(\mathcal{R})$ As $\mathit{Gal}(F(a)/F)$ acts simply transitivity on $\mathcal{R}$ we have $|\mathit{Gal}(F(a)/F)| = |\mathcal{R}|$ with $|\mathcal{R}| \leq \mathit{deg}(f) = n$* ■

Example 2.1.2 *1) $\mathit{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ we have the minimal polynomial of $\sqrt{3}$) is x^2-3 so x^2-3 has two roots in $\mathbb{Q}(\sqrt{3})$ so $|\mathit{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})| = 2$ so $\mathit{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, \tau\}$ with $\tau(\sqrt{3}) = -\sqrt{3}$*
2) $\mathit{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ we have the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ and this polynomial has one roots in $\mathbb{Q}(\sqrt[3]{2})$ so $|\mathit{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$ so $\mathit{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$
3) $\mathit{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, we have $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is splitting field of f over $\mathbb{Q}$ with $f(x) = (x^2 - 2)(x^2-3)$ then f have a 4 roots in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ so $|\mathit{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4$ and $\mathit{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{id, \tau_1, \tau_2, \tau_3\}$ with:

$$id: \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \quad \tau_1: \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \quad \tau_2: \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases} \quad \tau_3: \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases}$$

Definition 2.1.3 *A finite extension E/F is called galois extension if this extension is a normal and separable.*

Definition 2.1.4 *Let E/F be a Galois extension. If $a \in E$ the elements τa for $\tau \in \mathit{Gal}(E/F)$ are called the conjugates (or Galois conjugates) of a over F. If K is a subfield of E contains F, the field $\tau(E)$ is said the conjugate field of K over F.*

Corollary 2.1.1 *Let be E/F a Galois extension with $[E : F] = n$, then $\mathit{Gal}(E/F)$ is isomorphic to a subgroup of S_n and $\mathit{Gal}(E/F)$ acts simply transitively of the set of roots of the minimal*

polynomial and $|Gal(E/F)| = n$.

Proof.

As the E/F *is separable By the Theorem of the Primitive Element see (1.6.2) there is* $b \in E$ *such that* $E = F(b)$.

Let f *be the minimal polynomial of* b *over* F *As* E/F *is normal extension then* f *splits over* E *, and also the roots of* f *are distinct (because* E/F *is separable) so we define* $\mathcal{R} = \{a_1, a_2, ..., a_n\}$ *with* $|\mathcal{R}| = n$ *and by the Theorem (2.1.1)* $Gal(E/F)$ *is isomorphic to a subgroup of* S_n *and* $|Gal(E/F)| = |\mathcal{R}| = n$ ■

Proposition 2.1.1 *Let* E/F *be Galois extension we take* $a, b \in E$ *, So there is* $\varphi \in Gal(E/F)$ *with* $\varphi(a) = b$ *if and only if* a *and* b *has the same minimal polynomial over* F.

Proof.

The inverse implication, we have a *and* b *are roots of the minimal polynomial we denoted* f *and by the corollary (1.4.3) there exist a unique* F*-isomorphism* φ *s.t* $\psi : F(a) \to F(b)$ *with* $\psi(a) = b$ *,As* E/F *is normal hence* E *is splitting field of* f *over* $F(a)$ *and* E *is splitting field of* f *over* $F(b)$ *then by The Theorem (1.4.3) there exist isomorphism of splitting fields.* $\varphi : E \to E$ *with* $\varphi|_{F(a)} = \psi$ *so we have* $\varphi|_{F(a)}$=ψ*-*F *isomorphism then* $\varphi|_F = id$ *so* $\varphi \in Gal(E/F)$ *and as* $a \in F(a)$ $\varphi(a) = \varphi(a)|_{F(a)} = \psi(a)$ *so* $\varphi(a) = b$.

Conversely, Let f *be a minimal polynomial of* a *over* F *and* g *is the minimal polynomial of* b *over* F *then* $0 = \varphi(f(a)) = f(\varphi(a)) = f(b)$ *so* b *is a zero of* f *then* $g|f$*....(1)*

and the other hand in the same way a *is a zero of* g *thus* $f|g$*....(2)*

by (1) and (2) As f *and* g *are monic we get* $f = g$ ■

Definition 2.1.5 *Let* E/F *be Galois extension ,and let* G *be a subgroup of* $Gal(E/F)$ *we define:*

$$Fix(G) = \{a \in E \,|\varphi(a) = a \ , \ for\ all\ \varphi \in G\}$$

and also we denote $Fix(G) = E^G$.

Theorem 2.1.2 *Let* E/F *be galois extension then:*

$$Fix(Gal(E/F)) = F$$

Proof.

We have $Fix(Gal(E/F)) \supseteq F$ *is clearly because* $\varphi(a) = a$ *for all* $\varphi \in Gal(E/F)$.

Let $a \in Fix(Gal(E/F))$ so $\varphi(a) = a$ thus we take f be the minimal polynomial of a over F As E/F be a normal so f splits over E ,let b other roots of f so by the ***previous corollary*** *we have $\varphi(a) = b$ and by assumption $a = b$ so all roots of f are equals and the other hand E/F separable so the root of f is simple and we have f is monic hence $f(x) = x - a$ with $f \in F[x]$ finally $a \in F$*

■

Definition 2.1.6 *Let $f \in F[x]$ be noconstant polynomial , we consider E be a splitting Field of f over F ,we define $Gal(E/F))$ by:*

$$Gal(E/F) = Gal(f)$$

Proposition 2.1.2 *Let $f \in F[x]$ be noconstant polynomial with $deg(f) = n$,we take E the splitting field of f over F ,let $\mathcal{R}$ be a set of all roots of f in E ($\mathcal{R} \subset E$) then:*

(1) $Gal(f)$ is isomorphic to a subgroup of $S(\mathcal{R})$ and $|Gal(f)|$ divides $n!$.

(2) if all roots of f are simple then f is irreducible if and only if $Gal(f)$ acts transitively on $\mathcal{R}$.

Proof.

(1) Let E be a splitting field of f over F , we take the splitting field $E = F(\mathcal{R})$,we have E/F is a finite field extension with $Gal(E/F) = Gal(f)$, we take $\varphi \in Gal(E/F)$ and if $\alpha \in \mathcal{R}$ then $\varphi(f(\alpha)) = f(\varphi(\alpha)) = 0$ thus $\varphi(\alpha) \in \mathcal{R}$, we define a map $\Phi : Gal(E/F) \longrightarrow S(\mathcal{R})$ then we have Φ is a group homomorphism, we will proof Φ is injective, if we take $\varphi \in ker(\Phi)$ then $\varphi|_{\mathcal{R}} = id_{\mathcal{R}}$ and the other hand we have $\varphi|_F = id_F$ so $\varphi = id_E$ with $E = F(\mathcal{R})$ thus $ker(\Phi) = id_E$ hence Φ is injective, then $Gal(f)$ is isomorphic to a subgroup of $S(\mathcal{R})$ then $|Gal(f)|$ divides $|\mathcal{R}|!$ as $|\mathcal{R}| \leq n$ so $|\mathcal{R}|!$ divides $n!$ thus $|Gal(f)|$ divides $n!$.

(2) Assume that all roots of f are simple then f is minimal polynomial of $a, b \in \mathcal{R}$ so by the corollary (1.4.3) the exist a unique F-isomorphism $\psi : F(a) \to F(b)$ with $\psi(a) = b$, we have E is the splitting field of f over $F(a)$ and over $F(b)$ thus by The theorem (1.4.3) there exist an isomorphism φ such that $\varphi : E \longrightarrow E$ with $\varphi|_{F(a)} = \psi$ then $\varphi(a) = b$ so $\varphi \in Gal(E/F)$ Thus $Gal(f)$ acts transitively. on $\mathcal{R}$.

Conversely, Assume that $Gal(f)$ acts transitively on the roots of f and f is reducible in $F[x]$ then we want to show f has a multiple roots , we have f is reducible in $F[x]$ thus f has at least two different irreducible factors $f_1, f_2 \in F[x]$ with $f_1 f_2 | f$ Let α_1 be a root of f_1 in E and α_2 be a root of f_2 in E since $Gal(f)$ acts transitively on $\mathcal{R}$ thus there exist a $\varphi \in Gal(f)$ with $\varphi(\alpha_1) = \alpha_2$ so we have $\varphi(f_1(\alpha_1)) = f_1(\varphi(\alpha_1)) = f_1(\alpha_2) = 0$ so α_2 is a zero of f_1 in the same way α_1 is a root of

f_2 and f_1, f_2 are the minimal polynomials of α_1, α_2 so $f_1 = f_2$ so $f_1^2 | f$ thus f has a multiple root.

■

Remark 2.1.1 *Let E/F be a galois extension with E is the splitting field of f over F So we can find Gal(f) by two different ways:*

(1) if $\mathcal{R}$ is the set of roots of f in E then Gal(f) is isomorphic to a subgroup of $S(\mathcal{R})$.

(2) As E/F be galois extension by the Theorem of the primitive element there an element $a \in E$ such that $E = F(a)$, we take g be the minimal polynomial of a over F ,let be $\mathcal{M}$ be the set of zeros of g in E thus:

$$deg(g) = [E : F] = |\mathcal{M}| = |Gal(F(a)/F)|$$

Let $m = deg(g)$ thus Gal(f) is isomorphic to a (with $m = [E : F] \leq n!$) subgroup of S_m with Gal$(f) =$ Gal(E/F) which Gal(f) acts simple transitively on $\mathcal{M}$.

the second way is difficult to study galois group because it is very difficult to find primitive element and it is also very difficult to find the minimal polynomial of the primitive element.

Example 2.1.3 *(1) Let $f(x) = x^4 + 1 \in \mathbb{Q}[x]$ if α be a roots of f then $-\alpha, 1/\alpha, -1/\alpha$ are roots of f, since f is irreducible so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(f) = 4$ so $|Gal(f)| = 4$ (because the $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois extension) ,we claim that Gal$(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ we take $\tau, \sigma \in$ Gal(f) with $\tau(\alpha) = -\alpha$ and $\sigma(\alpha) = 1/\alpha$ and we can see $\sigma\tau = \tau\sigma$ and $\sigma^2 = \tau^2 = id$,*

thus Gal$(f) \cong \langle \tau, \sigma \rangle$ As $|Gal(f)| = 4$ we get Gal$(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (this group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a called Klein 4-group).

(2) Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ the we have $\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)$ be a splitting field of $\mathbb{Q}$ we found $\left[\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right) : \mathbb{Q}\right] = 6$ because it is is a galois extension and the number of roots of f in $\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)$ is three so Gal(f) is isomorphic of a subgroup of S_3 , thus Gal$(f) \cong S_3$.

2.2 The Fundamental Theorem of Galois Theory

The fundamental theorem of Galois theory says there is a relation between the intermediate fields L of a Galois extension E/F to the subgroups of the Galois group Gal(E/F).

Definition 2.2.1 *Let be E/F be galois extension ,Let H be a subgroup of Gal(E/F) we define the fixed field of H*

$$Fix(H) = \{a \in E \mid \varphi(a) = a \text{ ,for all } \varphi \in H\}$$

then clearly Fix(H) is a subfield of E contains F or the intermediate fields of E/F
by The theorem (2.1.2) we see :

$$Fix(Gal(E/F)) = F$$

Remark 2.2.1 *(1) If L be an intermediate field of E/F then*

$$Gal(E/L) = \{\varphi \in Gal(E/F) \mid \varphi|_L = id\}$$

Gal(E/L) is a subgroup of Gal(E/F).
(2) If you give a subgroup of Gal(E/F) we can associated by the intermediate fields of E/F, Conversely if we have an intermediate fields of E/F we can associated a subgroups of galois group Gal(E/F) , we say this two operations are bijections then there is the correspondence between the subgroups and the intermediate fields we called it the correspondence of galois the next theorem we will see it.

Theorem 2.2.1 *(The Fundamental theorem of Galois theory) Let be E/F be galois extension with $G =$ Gal(E/F) Then there is a bijection:*

$$\{\text{subgroups of } G\} \rightleftarrows \{\text{The intermediate fields of } E/F\}$$

(1) by the two maps (correspondence) $H :\to$ Fix(H) and $L \to$ Gal(E/L) i.e:
Fix(Gal$(L/F)) = F$ and Gal$(E/$Fix$(H)) = H$.
(2) $[E :$ Fix$(H)] = |H|$ and $[$Fix$(H) : F] = [G : H]$ for subgroups H in G.
(3) $[E : L] = |$Gal$(E/L)|$ and $[L : F] = [G :$ Gal$(E/L)]$ for intermediate fields L.
Proof.
We will proof the part (1) the others (2) and (3) are result from (1)
Let L be an intermediate field of E/F we proof that if E/F is galois extension then E/L is also galois extension ,As E/F is galois extension then E is a splitting field of some $f \in F[x]$ then

then E is also a splitting field of f over L so E/L is a normal extension, Let g be the minimal polynomial of $a \in E$ over F ,let hbe the minimal polynomial of $a \in E$ over L, since E/F is separable so all roots of g are simple and the other hand we have $h(a) = 0$ so h divides g thus h has no multiple roots in E so E/l is separable then E/L is galois extension and by the The theorem (2.1.2) we have Fix $(Gal(E/L)) = L$.

We will proof the second part of (1) Let H be a subgroup of $Gal(E/F)$ then we will show $Gal(E/Fix(H)) = H$ with $L = Fix(H)$ By the theorem of the primitive element there is an element $a \in E$ such that $E = F(a)$,Let f be a minimal polynomial of a over F we define f: $f(x) = \prod_{\varphi \in H}(x - \varphi(a)) \in E[x]$ with degree $|H|$, we have all roots of f are distinct, if we take $\varphi(a) = \psi(a)$ $\varphi, \psi \in H$ with $\varphi \notin \psi$ thus $(\varphi \circ \psi^{-1})(a) = a$ then $\varphi = \psi$ Impossible so all roots of f are distinct.

we can write $f = \sum_{i=1}^{|H|} b_i x^i$ $b_i \in E[x]$ we will show that $f \in L[x]$ ie $\forall i$ let $\psi \in H$ so

$$\psi(f) = \sum_{i=1}^{|H|} \psi(b_i)x^i = \prod_{\varphi \in H}(x - \psi(\varphi(a))) = \prod_{\varphi \in H}(x - \varphi(a))$$

so for all $\psi \in H$ we have $\psi(b_i) = b_i$ so $b_i \in L$ then $f \in L[x]$, we have $fa) = 0$ thus we take g the minimal polynomial of a over L so $g|f$ and we have $E = F(a) = L(a)$ (because E is the smallest contain a and L) thus:

$$|Gal(E/L)| = [E : L] = deg(g) \leq |H| = deg(f)$$

and the other hand clearly $Gal(E/L) \supset H$ ($L = Fix(H)$) so $Gal(E/L) = H$

(2) we have $Gal(E/Fix(H)) = H$ so $|Gal(E/Fix(H))| = |H|$. ■

Notation 2.2.1 *Let L be intermediate field of E/F let $\sigma \in Gal(E/F)$ with $\sigma(L) = \{\sigma(a) \mid a \in L\}$ it is clearly $\sigma(L)$ is an intermediate field of E/F.*

Lemma 2.2.1 *Let L is an intermediate field of Galois extension E/F ,let $\sigma \in Gal(E/F)$ then*

$$Gal(E/\sigma(L)) = \sigma Gal(E/L)\sigma^{-1}$$

Proof.

Let $\varphi \in Gal(E/F)$ then $\varphi \in Gal(E/\sigma(L)) \iff \varphi(\sigma(a)) = \sigma(a)$ $\forall a \in L \iff (\sigma^{-1}\varphi\sigma)(a) = a$ $\forall a \in L$ so we have $\sigma^{-1}\varphi\sigma \in Gal(E/L)$ if and only if $\varphi \in \sigma Gal(E/L)\sigma^{-1}$ ■

Theorem 2.2.2 *Let E/F is a Galois extension and let L is an intermediate field of E/F then The following are equivalent:*

(1) L/F is a normal extension.

(2) $\sigma(L) = L$ for every $\sigma \in Gal(E/F)$.

(3) $Gal(E/L)$ is a normal subgroup of $Gal(E/F)$.

Proof.

"(1) $\Longrightarrow$ (2)" Assume that L/F is a normal extension let $\sigma \in Gal(E/F)$ $a \in F$,let f be the minimal polynomial of a in L ,As L/F is a normal then f splits over L and we have $f(\sigma(a)) = \sigma(f(a)) = 0$ then $\sigma(a)$ is a zero of f thus $\sigma(a) \in L$ (we now that $\sigma(a) \in \sigma(L)$) so $\sigma(L) \subset L$,the other inclusion by the same way for σ^{-1} we get $\sigma^{-1}(L) \subset L \Longrightarrow L \subset \sigma(L)$

"(2) $\Longrightarrow$ (3)" we take $\sigma \in Gal(E/F)$ then we take by assumption $\sigma(L) = L$ so we get

$$\sigma Gal(E/L)\sigma^{-1} = Gal(E/\sigma(L)) = Gal(E/L)$$

thus $Gal(E/L) \lhd Gal(E/F)$.

"(3) $\Longrightarrow$ (1)" Let $f \in F[x]$ be irreducible polynomial and let $a \in L$ with $f(a) = 0$ we wiil proof f splits over L but firstly we have $Gal(E/L) \lhd Gal(E/F)$ thus

$$Gal(E/L) = \sigma Gal(E/L)\sigma^{-1} = Gal(E/\sigma(L))$$

hence by the fundamental theorem of Galois theory we have $\sigma(L) = L$,Let b be other root of f As E/F is a Galois extension there is $\varphi \in Gal(E/F)$ and since a and b are roots by same minimal polynomial f we get $\varphi(a) = b$ since $\forall \sigma \in Gal(E/F)$ we have $\sigma(L) = L$ In particular $\varphi(L) = L$ we have $b \in L$ hence all roots in L thus f splits over L ■

Corollary 2.2.1 *Let E/F be galois extension and let L be an intermediate field of E/F then:*
if L/F be a normal extznsion we have

$$Gal(L/F) \cong Gal(E/F)/Gal(E/L)$$

Proof.

We take $\sigma \in Gal(E/F)$ then $\sigma(L) = L$ Thus $\sigma_L \in Gal(L/F)$ so we define a map $\psi : Gal(E/F) \to Gal(L/F)$ by $\sigma \to \sigma_L$ so ψ group is a homomorphism and the kernal is $Gal(E/L)$ hence Thus by the isomorphism theorem of groups then $Gal(E/F)/Gal(E/L)$ is isomorphic of subgroupd of $Gal(L/F)$ and the other hand we have

$$|Gal(E/F)/Gal(E/L)| = [E : F]/[E : L]$$

and by the degree theorem we have $[E : F]/[E : L] = [L : F] = |Gal(L/F)|$
so $Gal(L/F) \cong Gal(E/F)/Gal(E/L)$ ■

Example 2.2.1 *The splitting field of* $x^3 - 2$ *in* $\mathbb{Q}$ *is* $\mathbb{Q}(\sqrt[3]{2}, \omega)$ *with* $\omega = e^{2\pi i/3}$ *and we define* τ *and* σ *with* $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ *and* $\tau(\omega) = \omega^2$, $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ *and* $\sigma(\omega) = \omega$ *so we have* $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ *in this figure (2.2) we have the diagramme of subgroups of* $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ *and the diagramme of subfield of* $\mathbb{Q}(\sqrt[3]{2}, \omega)$*, Also, corresponding subgroups and subfields are in corresponding positions for example* $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2}))$ *is* $\{1, \tau\}$

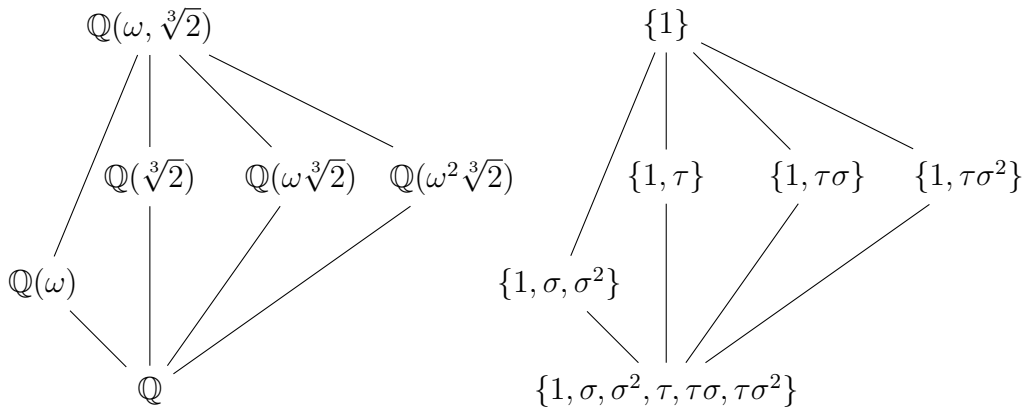

Figure 2.1: Figure

Chapter 3

Applications

3.1 Solvability by radicals

we have a semilar formula to solution for equation of degree 2 *and* 3 *and* 4 *but nobody found for degree* 5.
Abel proved that there is no formula for degree 6 *in this chapter Let* E *be a field of of characteristic* 0.

Definition 3.1.1 *Let* E/F *be a field extension,* E/F *is called a radical extension if there is a chain*

$$E = L_n \supset L_{n-1} \supset \ldots \supset L_0 = F$$

of of intermediate fields where $a_1^{m_1} \in F$ *and* $L_{i+1} = L_i(a_i)$ *and* $a_i^{m_i} \in L(a_1, a_2, ..., a_{_{i-1)}}$ *, where* a_i *is a zero of* $x^{n_i} - b_i$ *for some* $b_i \in, L_i$.

Example 3.1.1 $\mathbb{Q}(\sqrt{2})$ *be a radical extension of* $\mathbb{Q}$.

Definition 3.1.2 *we call* $f \in F[x]$ *is solvable by radical if* f *there exist a radical extension* E/F *and* f *splits over* E.

Proposition 3.1.1 *Let* E/F *be a radical extension. Then* E *is contained in a radical extension* E' *of* F *such that* E'/F *is a Galois extension.*

Definition 3.1.3 *A group* G *is called solvable if there exist a chain of subgroups*

$$G = G_0 \supset G_1 \ldots\ldots \supset G_n = \{1\}$$

such that for all i G_i is a subgroup of G and G_{i+1} is a normal of G_i and G_i/G_{i+1} is abelian group.

Example 3.1.2 *S_3 is solvable , because xe have $< (123) >$ is a normal subgroup of S_3 and we have $S_3/ < (123) > \cong \mathbb{Z}_2$.*

Definition 3.1.4 *Let G be a group wuth $a, b \in G$ we define The commutator of a, b by $[a, b] = a^{-1}b^{-1}ab$, if $[a, b] = 1$ if and only if $ab = ba$, we define The commutator subgroup of G we denoted G' such that G' is the subgroup generated by The commutator $[a, b]$ with $G' = \{[a, b] \,|\, a, b \in G\}$ and they evident if G is abelian if and only if $G' = \{1\}$.*

Notation 3.1.1 *The subgroup of G generated by a finite set $S \subset G$ defined by*

$$\langle S \rangle = \left\{ a_1 ... a_n \,|\, n \in \mathbb{N},\ a_i \text{ or } a_i^{-1} \in S \right\}$$

Lemma 3.1.1 *(1) G' is a normal subgroup of G*

(2) G/G' is abelian.

(3) If H is a normal subgroup of G with G/H is abelian we get $H \supset G'$.

Definition 3.1.5 *Let G be a group we define $G^{(1)} = G'$ and by induction we have $\left(G^{(n)}\right)' = G^{(n+1)}$ with $G^{(n+1)}$ is a normal subgroup of $G^{(n)}$ and $G^{(n)}/G^{(n+1)}$ be abelian.*

Lemma 3.1.2 *G is a solvable if and only if $G^{(n)} = \{1\}$.*

Proof.

Assume that $G^{(n)} = \{1\}$ we have a chain of subgroups

$$G = G^{(0)} \supset G^{(1)} \ldots \supset G^{(n)} = \{1\}$$

and for all i $G^{(i+1)}$ is normal subgroup of $G^{(i)}$ and $G^{(i)}/G^{(i+1)}$ is abelian by the previous lemma thus G is a solvable.

Conversely Assume that G is solvable then we have a chain of subgroups in G

$$G = H_0 \supset H_1 \ldots \supset H_n = \{1\}$$

with H_{i+1} is normal of H_i and H_i/H_{i+1} is abelian so by the previous lemma we have $H_{i+1} \supset H_i'$ so $H_1 \supset G'$ and $H_2 \supset H_1' \supset G'' = G^{(2)}$ then by induction we get $\{1\} = H_n \supset G^{(n)}$ so $G^{(n)} = \{1\}$ ■

Corollary 3.1.1 *Let G be solvable group and $\varphi : G \to H$ is a surjective group homomorphism. Thus H is solvable.*

Proof.

Let $a, b \in G$ $\varphi([a,b]) = [\varphi(a), \varphi(a)]$ as φ is a surjective then $H' = \varphi(G')$ there for we find for all i we have $H^{(i)} = \varphi(G'^{(i)})$ As a G is solvable there is $n \in \mathbb{N}$ $G'^{(n)} = \{1\}$ and $\varphi(G'^{(n)}) = H^{(n)} = \{1\}$ ■

Definition 3.1.6 *Let $n \in \mathbb{N}$,Let E be a field an element $\eta \in E$ s called an n-th root of unity if $\zeta^n = 1$,It is called a primitive n-th root of unity if $\zeta^n = 1$ and for $0 < i < n$ then $\zeta^i \neq 1$.*

Lemma 3.1.3 *Let $n > 0$ we take F a field with char$(F) = 0$,let ζ be a primitive element n^{th} root of unity in extension field of F thus $F(\zeta)/F$ is a galois extension , the galois group Gal $(F(\zeta)/F)$ is abelian.*

Proof.

We have $F(\zeta)$ is a splitting field of $x^n - 1$ over F , we consider the set $A = \{\zeta^s \mid 0 \leq s \leq n-1\}$ are roots of $x^n - 1$,we have $A \neq \varnothing$ because $1 \in A$, so all roots are distincts because if $\zeta^i = \zeta^j$ for $i < j \leq n-1$ thus $\zeta^{j-1} = 1$ then $i = j$ so all roots of $x^n - 1$ are distincts so we can write of this formula

$$x^n - 1 = (x-1)(x-\zeta)\dots\left(x-\zeta^{n-1}\right)$$

and we have obtained this field extension by add the roots of of this polynomial $x^n - 1$ thus $F(\zeta)$ is a splitting field of $x^n - 1$ over F so $F(\zeta)/F$ is normal extension and as char$(F) = 0$ so $F(\zeta)/F$ is a galois extension,

Let $G =$ Gal $(F(\zeta)/F)$ we will see that G is is abelian, if $\sigma \in G$ then $\sigma(\zeta)$ is roots of $x^n - 1$ so we can write $\sigma(\zeta) = \zeta^j$ for some $j \in 0, 1..., n-1$ As G is a subgroup of permutation of a set $\{1, \zeta, ..., \zeta^{n-1}\}$ thus if $\sigma, \tau \in G$ then $\sigma(\zeta) = \tau(\zeta)$ then $\sigma = \tau$

we take $\sigma, \tau \in G$ with $\sigma(\zeta) = \zeta^i$ and $\tau(\zeta) = \zeta^j$ so

$$(\sigma\tau)(\zeta) = \sigma\left(\zeta^j\right) = \sigma(\zeta)^j = \left(\zeta^i\right)^j = \zeta^{ij}$$

and by the same way we get $(\tau\sigma)(\zeta) = \zeta^{ij}$ Thus $\sigma\tau = \tau\sigma$ then G is abelian ■

Theorem 3.1.1 *Let $n > 0$ let F be field contains a primitive n-th root of unity, let $a \in F - \{0\}$,let E be a splitting field of $x^n - a$ over F.*

(1) $E = F(\alpha)$ such that α is a root of $x^n - a$.

(2) Gal(E/F) is abelian.

Proof.

(1) α is a root of $x^n - a$, Let ζ is the primitive n-th root of unity then $\alpha, \zeta\alpha, ..., \alpha^{n-1}\alpha$ are roots of $x^n - a$ and distincts because if we take $\zeta^i\alpha = \zeta^j\alpha$ then $(\zeta^i - \zeta^j)\,\alpha = 0$ since $\alpha \neq 0$ thus $\zeta^i = \zeta^j$ so $i = j$ for $0 \leq i < j \leq n$ so E/F is splitting field of $x^n - a$ over F

(2) Let $\sigma, \tau \in$ Gal(E/F) we we have $\sigma(\zeta^i\alpha) = \zeta^i\sigma(\alpha)$ because $\zeta^i \in F$ so $\sigma(\alpha) = \zeta^s\alpha$ and $\tau(\alpha) = \zeta^t\alpha$ then

$$(\sigma\tau)(\alpha) = \sigma\left(\zeta^t\alpha\right) = \zeta^t\sigma(\alpha) = \zeta^{s+t}\alpha$$

and by the same way way we get $(\tau\sigma)(\alpha) = \zeta^{t+s}\alpha$ thus $\sigma\tau = \tau\sigma$ thus Gal(E/F) is abelian ■

.

Theorem 3.1.2 *(Galois) Let F be a field of Char$(F) = 0$, let $f \in F[x]$ thus f is solvable by radicals if end only if Gal(f) is solvable.*

Example 3.1.3 *The polynomial $x^5 - 2$ is irreducible and degree 5 is solved by radicals because the Galois group is solvable and the field extension looks:*

$$\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \sqrt[5]{2})$$

Proposition 3.1.2 *Let $f \in F[x]$ with deg$(f) \leq 4$ then f is solvable by radical.*

Remark 3.1.1 *For $n \geq 5$. S_n is not solvable , we have for $n \geq 5$ then A_n is simple (i.e the only normal subgroups of A_n are $\{1\}$ and A_n) and nonabelian group so we have the series of the subgroups*

$$S_n \triangleright A_n \triangleright \{1\}$$

with $S_n/A_n \cong \mathbb{Z}_2$ and $A_n/\{1\} \cong A_n$ but we have A_n is nonabelian group so S_n is not solvable for $n \geq 5$

Theorem 3.1.3 *Let p be a prime number Let $f \in \mathbb{Q}[x]$ is an irreducible polynomial with degree p if f has $p - 2$ roots in $\mathbb{R}$ then Gal$(f) \cong S_5$.*

Example 3.1.4 *Let $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ by the Eisenstein criterion f is irreducible over $\mathbb{Q}[x]$ for $p = 3$ and by the intermediate value theorem f has three roots in $\mathbb{R}$ so Gal$(f) \cong S_5$ so f f is not solvable by radicals.*

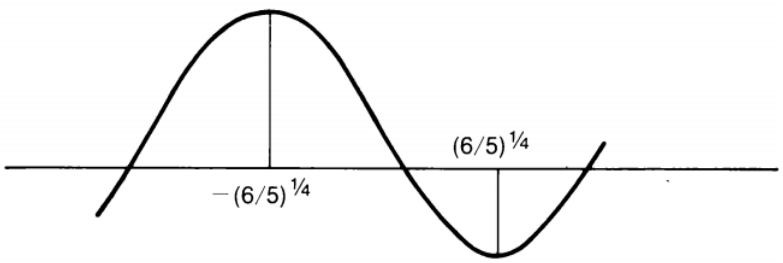

Figure 3.1: Graph of $x^5 - 6x + 3$

Conclusion

In this work we have studied some concepts of Galois extension of a commutative field. After giving some properties we give an application of this theory to the problem of solving algebraic equation in one unknown of degree greater then 5, by radicals.

Bibliography

[1] ***David S. Dummit, Richard M. Foote*** ,Abstract Algebra,*Third eddition,Wiley and Sons 2003.*

[2] ***John R.Durbin,*** Modern Algebra An Introduction *sixth Eddition ,Wiley and Sons 2006* .

[3] ***Larry Joel Goldstein,*** Abstract Algebra A First Course *Prentics-hall Inc Englewood Cliffs New jersey,1973.*

[4] ***Lothar Gottsche*** ,Introduction to Algebra.

[5] ***Richard Borcherds*** *,* Course Algebra *, fall 2017.*

الملخص:

الهدف من هذا العمل هو مقدمة حول توسيعات غالوا لحقل تبديلي و بعض التطبيقات لها :حل المعادلات الجبرية بواسطة علامات الجذور. لذا العمل مكون من ثلاثة فصول : مجمل عن المهم في نظرية الحقول، توسيعات غالوا وتطبيق في حل المعادلات الجبرية بواسطة علامات الجذور.

الكلمات المفتاحية: توسيع الحقل، توسيع غالوا ، زمرة قابلة للحل، معادلة قابلة للحل بواسطة علامات الجذور.

Abstract:

The purpose of this work is to provide an introduction to Galois extension of a field and some of its applications: the solvability of equations by radicals. To achieve this purpose the work is divided into three chapters : summaries from the field theory, Galois extension and application to solvability of equations by radicals.

Keywords: field extension, Galois extension, solvable group, solvable equation by radicals.