



University of Bahrain
College of Science
Department of Mathematics
Second Semester 2005/2006

Galois Theory and Application

Done by: Abdulla Eid
abdullaeid@gmail.com

Supervised by: Dr. Samira Saidi

TABLE OF CONTENTS

ACKNOWLEDGMENT	i
ABSTRACT	ii
CHAPTER 1 FIELD THEORY	1
§ 1.1 Extension Fields	2
§ 1.2 Splitting Fields	15
§ 1.3 Separable Fields	25
CHAPTER 2 THE FUNDAMENTAL THEOREM OF GALOIS THEORY	31
§ 2.1 Automorphisms and Fixed Fields	32
§ 2.2 The Fundamental Theorem of Galois Theory	41
CHAPTER 3 APPLICATIONS	51
§ 3.1 Cyclotomic Extensions	52
§ 3.2 The Galois Group of a Cubic Polynomials	60
REFERENCES	65

Prepared by:
Abdulla Jaffer Eid
20024608
Supervised by:
Dr. Samira Al-Saidi

ACKNOWLEDGEMENT

While accomplishing this project I was blessed with a great assistance from Dr.Samira Al-Saidi who pushed me always to do my best and gave me a great knowledge to do whatever I had done. I am of course responsible for what is written in this documentation, but I have to acknowledge the work of Dr.Samira with me, which has greatly improved the quality of what I did. I was really lucky to work with her, I believed that I will learn a lot of new things just because she was my supervisor, she has a clear vision and a good idea of what I need.

My special thanks go to Dr. Abulsalam Almannai who was providing me with more information to improve my knowledge in order to produce a good project, he taught me not only mathematics but also how to analyze any statement and reach to prove it in a professional way.

I am grateful to Dr.Ali Khan who gives me the opportunity to prove my self and by that I was confident in my self that I can learn a lot of new things independently and I can write about them in an appropriate way.

I want to thank my fiend Mr.Hussain Abdulla who work hard with me while typing this project and do a lot of great job to have this project in this way.

Last but not the least I want to thank every one help me in doing my project and was patient on me especially my mother and my students.

ABSTRACT

Galois Theory is the connection between groups and fields, known as extension fields. This is what the project is about.

This project is divided into three chapters. In chapter 1 the theory of extension fields is introduced along with examples and related theorems. Special field extensions such as algebraic extensions which lay a major role in the subsequent work are introduced along with the splitting field of polynomials: these extension fields of the field of coefficients of a polynomial that contain all its roots. The existence and uniqueness of such fields was dealt with.

The problem of separability of polynomials was also treated in this chapter, that is when does a polynomial have distinct roots in some splitting field.

Chapter 2 is devoted to the fundamental theorem of Galois Theory. Talking first about the fixed field of a group of automorphisms of fields, defining Galois groups and normal extensions throughout, we reached to the famous theorem of Galois: the one to one corresponding between the intermediate fields of an extension field and the subgroups of its Galois group. Examples were presented to illustrate the results.

The applications of the fundamental theorem of Galois Theory are diverse the major one is the study of solvability of polynomial equation of any degree using formulas, like the well known formula, solving any quadratic polynomial equation. Unfortunately, and due to the lack of time, this application is not included in my project as I planned earlier but I shall look into it during my summer vacation. In chapter 3 two application are treated, the first is about cyclotomic extensions: the splitting fields of cyclotomic polynomials and the second is on the Galois group of a cubic polynomial over \mathbb{Q} .

The application of Galois Theory is not just in pure mathematics, it goes beyond that. We can use the galois fields (finite fields) in many areas of computer science especially in cryptography or more specific in DES (Data Encryption Standard) and AES (Advanced Encryption Standard). The use of these algorithms is widespread in many military and commercial agencies.

CHAPTER 1

Field Theory

In this chapter we will study special types of fields (recall that a field is an integral domain with unity where every element has a multiplicative inverse), we will study the relation of a field with its subfield called an extension field and examine some of its properties and theorems related to it. Then we will study fields associated with a polynomial called splitting fields and we will end this chapter by studying an interesting field extension called separable extension.

§ 1.1 Extension Fields

Definition

If E is a field containing the field F , then E is said to be an extension field of F .

Notation

Let $E|F$ denote that E is an extension field of F where $E|F$ is shorthand for “ E over F ”.

Examples

(1) since $\mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$, then $\mathbf{R}|\mathbf{Q}$, $\mathbf{C}|\mathbf{R}$ and $\mathbf{C}|\mathbf{Q}$ are all extensions fields, we referred this as a tower of fields.

(2) Every field E is an extension field of its prime subfield (this is the intersection of all subfield of E), in this case E is called the base field of the extension.

(3) if p is a prime integer and $q = p^m$ for some positive integer m , then we know that $\mathbf{Z}_p \subseteq \mathbf{Z}_q$, hence $\mathbf{Z}_q|\mathbf{Z}_p$ is also a field extension. ◀

Now let $E|F$ be any field extension, then under the field operation of E we can consider E as a vector space over F , where the elements of E are the “vectors” and the elements of F are the “scalars” and this lead us to the following definition.

Definition

Let $E|F$ be a field extension, the dimension of the vector space E over F is called the degree of the extension $E|F$ and it's denoted by $[E:F]$, if the degree of $E|F$ is finite i.e. $[E:F] < \infty$, then $E|F$ is called a finite field extension.

Examples

(1) Since $\{1, i\}$ is a basis for the field \mathbf{C} over \mathbf{R} , then $[\mathbf{C}:\mathbf{R}] = 2$ and then $\mathbf{C}|\mathbf{R}$ is a finite field extension.

(2) Consider the polynomial ring $F[x]$ over a field F where $F[x]$ is an integral domain, let E be the quotient field of $F[x]$, then the set $\{1, x, x^2, \dots, x^n, \dots\}$ are linearly independent over F (because if $a_0 + a_1x + \dots + a_nx^n = 0$, $a_i \in F, \forall i = 1, 2, \dots, n$, then $a_i = 0, \forall i$) and also it spans E , hence $[E:F] = \infty$ and $E|F$ is infinite field extension. ◀

Definition

Let $E|F$ be an extension field, a subfield L of E is called an intermediate field of $E|F$ if $F \subseteq L \subseteq E$, L is called a proper intermediate field if $F \subset L \subset E$.

We turn now to very important theorem in studying field theory which is the degree theorem.

Theorem (The Degree Equation)

If $E|F$ is a finite field extension and $K|E$ is a finite field extension, then $K|F$ is also a finite field extension and $[K:F]=[K:E][E:F]$.

Proof:

Suppose that $[K:E]=n$ and the set $\{ \alpha_i : i = 1, 2, \dots, n, \alpha_i \in K \}$ be a basis for $K|E$ and $[E:F]=m$ and the set $\{ \beta_i : i = 1, 2, \dots, m, \beta_i \in E \}$ be a basis for $E|F$,

Now let $b \in K$, $b = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n$, where $a_i \in E$, for all $i=1, 2, \dots, n$

and since $a_i \in E$, then $a_i = c_{i1}\beta_1 + c_{i2}\beta_2 + \dots + c_{im}\beta_m$ i.e. $a_i = \sum_{j=1}^m c_{ij}\beta_j$, so

$$b = \sum_{i=1}^n \left(\sum_{j=1}^m c_{ij}\beta_j \right) \alpha_i = \sum_{i,j} c_{ij} (\beta_j \alpha_i),$$

and so the mn vectors $\alpha_i\beta_j$ span K over F , now to show that $\alpha_i\beta_j$ are linearly independent and then it will be a basis for $K|F$,

Let $\sum_{i=1}^n \left(\sum_{j=1}^m c_{ij}\beta_j \right) \alpha_i = 0$, since α_i 's are linearly independent, then $\sum_{j=1}^m c_{ij}\beta_j = 0$ and

also since β_j 's are linearly independent $c_{ij} = 0$, for all $i=1, 2, \dots, n$, and $j=1, 2, \dots, m$.

hence $\{ \alpha_i\beta_j : i = 1, 2, \dots, n, j = 1, 2, \dots, m \}$ is the basis for $K|F$ and that

$$[K:F]=mn=[K:E][E:F]. \quad \blacksquare$$

Definition

Let $E|F$ be a field extension, let c_1, c_2, \dots, c_n be elements in E , then E is said to be finitely generated if $E=F(c_1, c_2, \dots, c_n)$, where $F(c_1, c_2, \dots, c_n)$ is the smallest subfield of E containing F and c_1, c_2, \dots, c_n .

Example

$\mathbb{Q}(\sqrt{3})$ is finitely generated subfield of \mathbb{R} , where $\mathbb{Q}(\sqrt{3})$ is the smallest subfield of \mathbb{R} containing \mathbb{Q} and $\sqrt{3}$. ◀

Definition

Let $E|F$ be a field extension, an element $c \in E$ is said to be algebraic over F if $f(c)=0$ for some nonzero polynomial $f(x) \in F[x]$, if c is not algebraic, then c is said to be transcendental element over F .

Remark

Every element $c \in F$ is algebraic over F since c will be a zero for $f(x)=x-c \in F[x]$.

Examples

(1) The element $\sqrt{3}$ in \mathbb{R} is algebraic over \mathbb{Q} because $\sqrt{3}$ is a root for $x^2 - 3 \in \mathbb{Q}[x]$.

(2) The element i in \mathbb{C} is algebraic over \mathbb{Q} because i is a zero for $x^2 + 1 \in \mathbb{Q}[x]$.

(3) The real number e is algebraic over \mathbb{R} because e is a zero for $(x - e) \in \mathbb{R}[x]$, however e can be shown to be a transcendental element over \mathbb{Q} .
(Look at the end of this chapter for the existence of transcendental elements in \mathbb{R} over \mathbb{Q})

(4) $\sqrt{2 + \sqrt{5}}$ is algebraic element over \mathbb{Q} because $\sqrt{2 + \sqrt{5}}$ is a zero for $x^4 - 4x^2 - 1 = 0$. ◀

Theorem

Let $E|F$ be a field extension and $c \in E$, if c is algebraic over F , then c is a root for some nonzero unique irreducible monic polynomial $p(x)$ over F , furthermore if $f(x) \in F[x]$ such that $f(c)=0$, then $p(x) | f(x)$.

Proof:

Let $E|F$ be a field extension and $c \in E$. suppose c is algebraic element over F , consider the evaluation homomorphism $\phi_c : F[x] \rightarrow E$, where $\phi_c(x) = c$ and $\phi_c(a) = a$ for all $a \in F$, the kernel of ϕ_c is $\ker \phi_c = \{h(x) \in F[x] : \phi_c(h(x)) = 0\}$, $\ker \phi_c = \{h(x) \in F[x] : h(c) = 0\}$, since $F[x]$ is principle ideal domain, then the kernel of ϕ_c is generated by a nonzero polynomial in $F[x]$, therefore

$\ker \phi_c = (p(x))$, where $p(c)=0$ and $\deg p(x) \geq 1$, now let $f(x)$ be a nonzero polynomial in $F[x]$, such that $f(c) = 0$, then $f(x) \in \ker \phi_c$, then $f(x) \in (p(x))$. Hence $p(x) \mid f(x)$ and thus $p(x)$ is a polynomial with minimal degree ≥ 1 having c as a zero and any other nonzero polynomial $h(x)$ having c as a zero in $F[x]$ of the same degree as $p(x)$ will be of the form $h(x) = a p(x)$, where $a \in F$. so by multiplying by a suitable constant in F , we can assume $p(x)$ is monic polynomial, then $p(x)$ is a unique monic polynomial having c as a zero.

Now for the irreducibility, suppose $p(x) = u(x)v(x)$, where $u(x), v(x)$ has a lower degree than $p(x)$ and non-constant in $F[x]$, then $p(c) = u(c)v(c) = 0$, which implies that $u(c) = 0$ or $v(c) = 0$, since $F[x]$ is an integral domain, which contradict the fact that $p(x)$ is the polynomial with minimal degree having c as a zero, therefore $p(x)$ is irreducible monic polynomial. ■

Definition

Let $E \mid F$ be a field extension and $c \in E$ is an algebraic element over F , then the unique monic polynomial $p(x)$ having the property in the previous theorem is called the irreducible polynomial for c over F and will be denoted by $\text{irr}(c, F)$ and the degree of $\text{irr}(c, F)$ is the degree of c over F denoted by $\deg(c, F)$.

Example

(1) In $\mathbf{R} \mid \mathbf{Q}$ we have :

- i) $\text{irr}(\sqrt{3}, \mathbf{Q}) = x^2 - 3$ of degree 2 i.e. $\deg(\sqrt{3}, \mathbf{Q}) = 2$.
- ii) $\text{irr}(i, \mathbf{Q}) = x^2 + 1$ of degree 2 i.e. $\deg(i, \mathbf{Q}) = 2$.
- iii) $\text{irr}(\sqrt{3}, \mathbf{R}) = x - \sqrt{3}$ of degree 1 i.e. $\deg(\sqrt{3}, \mathbf{R}) = 1$.
- iv) $\text{irr}(\sqrt{2 + \sqrt{5}}, \mathbf{Q}) = x^4 - 4x^2 - 1$ of degree 4 i.e. $\deg(\sqrt{2 + \sqrt{5}}, \mathbf{Q}) = 4$.

Theorem

Let $E \mid F$ be a field extension, let $c \in E$ be algebraic element over F , then $\phi_c[F[x]] \cong \frac{F[x]}{(\text{irr}(c, F))}$, where $\phi_c : F[x] \rightarrow E$ is the evaluation homomorphism.

We shall denote this subfield of E by $F(c)$, where $F(c)$ is the intersection of all subfields of E containing both F and c , hence $F(c)$ is the smallest subfield containing F and c .

Definition

Given $E | F$ and $c \in E$, then the image of ϕ_c is called the simple field extension of F with a primitive element c , moreover this extension is the smallest subfield of E containing both c and F .

Theorem

Let $E | F$ be a field extension and $c \in E$, then $F[c]=F(c)$ if and only if c is algebraic over F .

Proof:

Let $E | F$ be a field extension, $c \in E$ is algebraic over F , then by the first isomorphism theorem, $F[c] \cong F[x]/(\text{irr}(c, F)) \cong F(c)$, since $F[x]/(\text{irr}(c, F))$ is a field because $(\text{irr}(c, F))$ is maximal ideal and because $F[c] \subseteq F(c)$, then $F[c]=F(c)$.

Conversely, suppose $F[c]=F(c)$, then if $c=0$ it will be a root for $x \in F[x]$, so suppose $c \neq 0$, then $c^{-1} \in F(c)$, then $c^{-1} = a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0$, where $a_i \in F, i = 0, 1, 2, \dots, n$, then $1 = a_n c^{n+1} + a_{n-1} c^n + \dots + a_1 c^2 + a_0 c$ and so $a_n c^{n+1} + a_{n-1} c^n + \dots + a_1 c^2 + a_0 c - 1 = 0$, hence c is algebraic over F . ■

Theorem

Let $E | F$ be a field extension and let $c \in E$ be an algebraic element over F of degree n , then $\{1, c, c^2, \dots, c^{n-1}\}$ is a basis for $F(c)$, equivalently every a in $F(c)$ can be expressed uniquely in the form $a = a_n c^{n-1} + a_{n-1} c^{n-2} + \dots + a_2 c + a_1, a_i \in F$.

Proof:

Let $E | F$ be a field extension and $c \in E$ be an algebraic element over F of degree n , now let $p(x)=\text{irr}(c, F)$, then $p(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$ So $p(c)=0$, then

$$c^n = -a_{n-1} c^{n-1} - a_{n-2} c^{n-2} - \dots - a_1 c + a_0$$

$$c^{n+1} = -a_{n-1} c^n - a_{n-2} c^{n-1} - \dots - a_1 c^2 + a_0 c$$

$$c^{n+1} = -a_{n-1}[-a_{n-1} c^{n-1} - a_{n-2} c^{n-2} - \dots - a_1 c + a_0] - a_{n-2} c^{n-1} - \dots - a_1 c^2 + a_0 c$$

·
·
·

$$c^{n+k} = -a'_{n-1}c^{n-1} - a'_{n-1}c^{n-2} - \dots - a'_1c + a'_0$$

So $\{1, c, c^2, \dots, c^{n-1}\}$ span $F(c) | F$.

for uniqueness, suppose $a \in F(c)$, then

$$a = a_0 + a_1c + \dots + a_{n-1}c^{n-1} = a'_0 + a'_1c + \dots + a'_{n-1}c^{n-1}, \text{ then}$$

$$(a_0 - a'_0) + (a_1 - a'_1)c + \dots + (a_{n-1} - a'_{n-1})c^{n-1} = 0, \text{ let}$$

$$g(x) = (a_0 - a'_0) + (a_1 - a'_1)x + \dots + (a_{n-1} - a'_{n-1})x^{n-1} \in F[x], \text{ then } g(c) = 0$$

and since $\deg g(x) < \deg p(x)$, then $g(x) \equiv 0$.

so $a_i = a'_i \quad \forall i = 0, 1, 2, \dots, n-1$ and hence $\{1, c, c^2, \dots, c^{n-1}\}$ is a basis for $F(c)$. ■

Corollary

Let $E | F$ be a field extension, if $c \in E$ is algebraic over F and of degree n , then $[F(c) : F] = n$.

Examples

(1) In $\mathbf{R} | \mathbf{Q}$, since $\deg(\sqrt{3}, \mathbf{Q}) = 2$, then $\{1, \sqrt{3}\}$ is a basis for $\mathbf{Q}(\sqrt{3}) | \mathbf{Q}$ and $\mathbf{Q}(\sqrt{3}) = \{q_0 + q_1\sqrt{3} : q_0, q_1 \in \mathbf{Q}\}$ and $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$.

(2) In $\mathbf{R}(i) | \mathbf{R}$, since $\deg(i, \mathbf{R}) = 2$, then $\{1, i\}$ is a basis for $\mathbf{R}(i)$, and $\mathbf{R}(i) = \{a + bi : a, b \in \mathbf{R}\}$ and also $[\mathbf{R}(i) : \mathbf{R}] = 2$.

(3) In $\mathbf{R} | \mathbf{Q}$, since $\sqrt[3]{3}$ is a root of $x^3 - 3 \in \mathbf{Q}[x]$, then $\deg(\sqrt[3]{3}, \mathbf{Q}) = 3$ and $\{1, \sqrt[3]{3}, (\sqrt[3]{3})^2\}$ is a basis for $\mathbf{Q}(\sqrt[3]{3})$, and also $[\mathbf{Q}(\sqrt[3]{3}) : \mathbf{Q}] = 3$. ◀

Now let us back to the degree equation and use it for the next examples.

Example

To find $[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}(\sqrt{2})]$, we apply the degree equation so $[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$, then $6 = 2[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}(\sqrt{2})]$ and hence $[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}(\sqrt{2})] = 3$.

and since $\{1, 2^{\frac{1}{6}}, 2^{\frac{2}{6}}, 2^{\frac{3}{6}}, 2^{\frac{4}{6}}, 2^{\frac{5}{6}}\}$ is a basis for $\mathbf{Q}(\sqrt[6]{2})$ over \mathbf{Q} and $\{1, 2^{\frac{1}{2}}\}$ is a basis for $\mathbf{Q}(\sqrt{2})$ over \mathbf{Q} , then by the same way in the proof of the degree equation, the set $\{1, 2^{\frac{1}{6}}, 2^{\frac{2}{6}}\}$ is a basis for $\mathbf{Q}(\sqrt[6]{2}) | \mathbf{Q}(\sqrt{2})$. ◀

Theorem

If $E | F$ be a field extension, $a, b \in E$ are algebraic elements over F , let $b \in F(a)$, then $\deg(b, F) | \deg(a, F)$.

Proof:

since $\deg(a, F) = [F(a):F]$, $\deg(b, F) = [F(b):F]$ and $F \subseteq F(b) \subseteq F(a)$ because $b \in F(a)$, then $[F(a):F] = [F(a):F(b)][F(b):F]$, hence $[F(b):F] | [F(a):F]$, hence $\deg(b, F) | \deg(a, F)$. ■

Example

There is no element of $\mathbf{Q}(\sqrt{3})$ that is a zero of $x^3 - 2$, because if there is such an element $b \in \mathbf{Q}(\sqrt{3})$ such that $b^3 - 2 = 0$, then $\deg(b, \mathbf{Q}) | \deg(\sqrt{3}, \mathbf{Q})$ and that means $3 | 2$ which is impossible. ◀

Recall from the field generated over F by a finite number of elements in E , (where $E | F$ is a field extension) is the smallest subfield of E containing F and these elements, the following lemma shows that this finitely generated field can be obtained recursively by a series of simple extensions.

Lemma

Let $E | F$ be a field extension, a and $b \in E$ are algebraic elements over F , then $F(a, b) = [F(a)](b)$.

Proof:

Since the field $F(a, b)$ contains F and a , then it contains $F(a)$ and because it contains also b it contains $F(b)$, so it contains $F(a)(b)$ and so $F(a)(b) \subseteq F(a, b)$ by minimality of the field $F(a)(b)$, and because $F(a)(b)$ contains F, a and b , then by the definition of $F(a, b)$, we have $F(a, b)$ is the smallest subfield of E containing F, a and b , therefore $F(a, b) \subseteq F(a)(b)$, hence $F(a, b) = F(a)(b)$.

Now in general,

if $E = F(c_1, c_2, \dots, c_n)$, where $c_i \in E, \forall i = 1, 2, \dots, n$, then $E = F(c_1, c_2, \dots, c_{n-1})(c_n)$

so let F_1 be the field generated over F by c_1

F_2 be the field generated over $F(c_1)$ by c_2

F_3 be the field generated over F_2 by c_3

.

.

F_i be the field generated over F_{i-1} by c_i

i.e. $F_{i+1} = F_i(c_{i+1})$, $i = 0,1,2,\dots,n-1$ and that $F_0 = F$
 so we will get the following chain : $F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = E$
 and by the degree equation we will get:
 $[E:F]=[E:F_n][F_n:F_{n-1}]\dots[F_1:F_0]$ ■

Example

To find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over \mathbb{Q} , we have $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over \mathbb{Q} and $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3})$ over \mathbb{Q} , then by the degree equation (in fact the result of its proof), we have the set $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3}) | \mathbb{Q}$.
 by the previous lemma, let $E=\mathbb{Q}(\sqrt{2})$, then $\mathbb{Q}(\sqrt{2}, \sqrt{3})=E(\sqrt{3})$, by the the degree equation $[E(\sqrt{3}):\mathbb{Q}]=[E(\sqrt{3}),\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$, hence $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$. ◀

Definition

A field extension $E | F$ is called algebraic if every element of E is algebraic over F , otherwise $E | F$ is called transcendental.

Examples

- (1) $\mathbb{C} | \mathbb{R}$ is algebraic because every nonzero polynomial in \mathbb{R} has a root in \mathbb{C}
- (2) $A | \mathbb{Q}$, where A is the set of all algebraic numbers in \mathbb{R} over \mathbb{Q} , the field A is called the field of algebraic numbers. ◀

Theorem

Every finite field extension $E | F$ is an algebraic extension.

Proof:

Assume $E | F$ is a finite field extension, let $[E:F]=n$, let $c \in E$.
 if $c=0,1$, then c is algebraic over F because $c \in F$.
 so assume $c \neq 0, c \neq 1$, then consider $\{1, c, c^2, \dots, c^n\}$, if they are not all distinct, then there exist $0 \leq i \neq j \leq n$ such that $c^i = c^j$, hence $c^{i-j} = 1$, then c is a root for $x^{i-j} - 1 \in F[x]$ and therefore c is algebraic.
 If $\{1, c, c^2, \dots, c^n\}$ are all of distinct elements, then they are linearly dependent because $[E:F]=n$, so there is b_0, b_1, \dots, b_n are not all zero, such that :
 $b_0 + b_1c + \dots + b_n c^n = 0$,
 hence c is a root for nonzero polynomial $f(x) = b_0 + b_1x + \dots + b_n x^n \in F[x]$

therefore c is algebraic over F . ■

Examples

(1) $\mathbb{Q}(\sqrt{3}) | \mathbb{Q}$ is algebraic extension because $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2 < \infty$

(2) $\mathbb{Q}(\sqrt{3}, \sqrt{2}) | \mathbb{Q}$ is algebraic extension because $[\mathbb{Q}(\sqrt{3}, \sqrt{2}):\mathbb{Q}]=4 < \infty$

(3) $\mathbb{R} | \mathbb{Q}$ is transcendental extension because there exist an element e such that e is not algebraic over \mathbb{Q} . ◀

Corollary

Let $E | F$ be a field extension, let $c \in E$, then c is algebraic over F if and only if $[F(c):F]=n$, where $n=\deg(c,F)$.

The next theorem is a summary of the results obtained about the simple extension $F(c)$.

Theorem

Let $E | F$ be a field extension, let $c \in E$ be an algebraic element over F , then the following are equivalent:

(1) $F(c)=F[c]$.

(2) $[F(c):F]=\deg(\text{irr}(c,F))$.

(3) $\{1, c, c^2, \dots, c^{n-1}\}$ is a basis of $F(c)$, where n is the degree of c over F .

(4) Every nonzero polynomial in $F[c]$ has an inverse in $F[c]$ and $(f(c))^{-1} = q(c)$, where $f(x)q(x)+p(x)r(x)=1$, where $p(x)=\text{irr}(c,F)$.

Proof (4):

Let $E | F$ be a field extension, $c \in E$ be an algebraic element over F , let $0 \neq f(x) \in F[x]$, such that $f(c) \neq 0$, then $p(x)=\text{irr}(c,F)$ doesn't divide $f(x)$, hence there is no common divisor between them, so $\gcd(f(x), p(x))=1$ (unit in F), so there exist $q(x), r(x)$ such that $f(x)q(x)+p(x)r(x)=1$ and so $f(c)q(c)+p(c)r(c)=1$, then $f(c)q(c)=1$, hence $(f(c))^{-1} = q(c)$.

the converse it straight forward that is if every polynomial $f(c)$ has an inverse in $F[c]$, then $F[c]$ is a field and thus $F[c]=F(c)$ and then c is algebraic. ■

Examples

In $\mathbb{C} | \mathbb{R}$, $i \in \mathbb{C}$ is an algebraic over \mathbb{R} , then

(1) $\mathbb{R}(i)=\{a+bi: a, b \in \mathbb{R}\}=\mathbb{R}[i]$.

(2) $[\mathbf{R}(i):\mathbf{R}] = \deg \text{irr}(i, \mathbf{R}) = \deg(x^2 + 1) = 2$.

(3) $\{1, i\}$ is a basis for $\mathbf{R}[i] | \mathbf{R}$.

(4) for $0 \neq f(i) \in F[i]$, $f(i) = a + bi$ has an inverse

$$(f(i))^{-1} = \frac{a^2 - b^2}{a^2 + b^2} - \frac{a^2 - b^2}{a^2 + b^2}i \in F[i]. \quad \blacktriangleleft$$

Remark

This theorem can be used to get similar results about finitely generated extensions as we will see in the following example.

Example

$\mathbf{Q}(\sqrt{3}, \sqrt{2}) | \mathbf{Q}$, $[\mathbf{Q}(\sqrt{3}, \sqrt{2}):\mathbf{Q}] = 4 < \infty$, then $\sqrt{3}, \sqrt{2}$ are algebraic over \mathbf{Q} (since $\sqrt{3}$ is algebraic over $\mathbf{Q}(\sqrt{2})$, then It will algebraic over \mathbf{Q}). ◀

Theorem

Let $E | F$ be a field extension, if L is the set of all algebraic elements of E over F , then L is an intermediate field of $E | F$.

Proof:

Suppose $E | F$ be a field extension, let $L = \{c \in E : c \text{ is algebraic over } F\}$, since $0, 1 \in L$, then $L \neq \emptyset$, now let $c \in F$, then c is algebraic over F , hence $F \subseteq L$, now let $a, b \in L$, since $a, b \in E$ are algebraic elements over F , then let $\deg \text{irr}(a, F) = n$ and $\deg \text{irr}(b, F) = m$, so we have $[F(a):F] = n$ and $[F(b):F] = m$, by the degree equation:
 $[F(a, b):F] = [F(a, b):F(a)][F(a):F]$, since $[F(a, b):F(a)] \leq m$, thus $[F(a, b):F]$ is finite, therefore $F(a, b) | F$ is finite field extension, hence every element of $F(a, b)$ is algebraic over F , since $a, b \in F(a, b)$, then $a - b \in F(a, b)$ and $ab^{-1} \in F(a, b)$, therefore $a - b$ and ab^{-1} are algebraic elements over F , hence $a - b, ab^{-1} \in L$, hence L is a subfield of E , so we have $F \subseteq L \subseteq E$ which shows that L is an intermediate field of $E | F$. ■

Examples

(1) The field of algebraic numbers A (A is the set of all real numbers which are zeros for nonzero polynomial over \mathbf{Q}).

(2) In the extension field \mathbf{C} over \mathbf{R} , the set of all algebraic elements in \mathbf{C} over \mathbf{R} is \mathbf{C} itself, we can prove that by using some knowledge from complex analysis

or specifically Liouville's theorem or we can use the degree equation again, where

$[C:\mathbf{R}] = [C:L][L:\mathbf{R}]$, since $i \in L$, therefore $L \neq \mathbf{R}$, hence $[L:\mathbf{R}] \neq 1$, therefore $2 = [C:L][L:\mathbf{R}]$, then $[C:L] = 1$ and thus $C = L$. ◀

Now one can ask if $L|F$ and $E|L$ are algebraic field extensions, then is $E|F$ also algebraic field extension where L is an intermediate field of $E|F$? the answer will be in the following theorem.

Theorem

Let L be an intermediate field of the field extension $E|F$, then $E|F$ is algebraic extension if and only if $E|L$ and $L|F$ are algebraic extensions.

Proof:

Let $E|F$ be a field extension, let L be an intermediate field of $E|F$, assume $E|F$ is algebraic extension, let $c \in E$, then c is a root for $\text{irr}(c,F) = p(x)$, since $F \subseteq L$, then $p(x) \in L[x]$, thus c is algebraic element over L also, and hence $E|L$ is algebraic extension. now let $c \in L$, then $c \in E$ and hence is algebraic over F , thus $L|F$ is algebraic extension.

therefore we proved that $E|F$ is algebraic extension only if $E|L$ and $L|F$ are algebraic extensions.

Conversely, suppose $E|L$ and $L|F$ are algebraic extensions, let $c \in E$, then c is a root for $\text{irr}(c,L) = p_L(x) = a_0 + a_1x + \dots + a_nx^n \in L[x]$, so c is algebraic over $F(a_0, a_1, \dots, a_n)$, now $F(a_0, a_1, \dots, a_n)(c) | F(a_0, a_1, \dots, a_n)$ is finite by (corollary in page 10).

Now

$$[F(a_0, a_1, \dots, a_n)(c):F] = [F(a_0, a_1, \dots, a_n)(c):F(a_0, a_1, \dots, a_n)][F(a_0, a_1, \dots, a_n):F]$$

since $F(a_0, a_1, \dots, a_n)$ are algebraic elements over F , therefore

$F(a_0, a_1, \dots, a_n)(c) | F$ is a finite extension, therefore c is algebraic over F , and this prove that $E|F$ is algebraic. ■

We know now that every finite extension is algebraic, but is the converse true? the answer is given in the following result about the field of algebraic numbers A .

Lemma

If p, p_1, p_2, \dots, p_n are distinct prime integers, then $\sqrt{p} \notin \mathbf{Q}(p_1, p_2, \dots, p_n)$

Proof:

proof by induction on n.

- Base case : $n=0$, then it is clear that $\sqrt{p} \notin \mathbf{Q}$

- Induction step :

assume $\sqrt{p} \notin \mathbf{Q}(p_1, p_2, \dots, p_k)$ and suppose $\sqrt{p} \in \mathbf{Q}(p_1, p_2, \dots, p_k, p_{k+1})$, then

$\sqrt{p} \in \mathbf{Q}(p_1, p_2, \dots, p_k)(p_{k+1})$, hence $\sqrt{p} = a + b\sqrt{p_{k+1}}$,

where $a, b \in \mathbf{Q}(p_1, p_2, \dots, p_k)$

now if $a=0$, then $\sqrt{p} = b\sqrt{p_{k+1}} \rightarrow p = b^2 p_{k+1}$, which is contradiction since p and p_{k+1} are distinct prime integers.

if $b=0$, then $\sqrt{p} = a \rightarrow p = a^2$ also a contradiction since p is prime integer.

so assume $a \neq 0, b \neq 0$, then $p = a^2 + 2ab\sqrt{p_{k+1}} + b^2 p_{k+1}$ i.e.

$\sqrt{p_{k+1}} = \frac{p - a^2 - b^2 p_{k+1}}{2ab} \in \mathbf{Q}(p_1, p_2, \dots, p_k)$, hence $p \in \mathbf{Q}(p_1, p_2, \dots, p_k)$ which a

contradiction with the induction hypothesis.

hence the result is true. ■

Theorem

$[A:\mathbf{Q}] = \infty$ and $A | \mathbf{Q}$ is algebraic extension.

Proof:

let $F = \mathbf{Q}(\{\sqrt{p} : p \text{ is prime integer}\}) \subset \mathbf{R}$, so by the previous lemma

$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subset \dots$

is a infinite strictly chain of intermediate field of $F | \mathbf{Q}$, hence $F | \mathbf{Q}$ must be infinite dimensional and hence $[F:\mathbf{Q}] = \infty$

now since the field of algebraic numbers A contain F , therefore $[A:\mathbf{Q}] = \infty$ and $A | \mathbf{Q}$ is algebraic extension and as a result, we have

$[R:\mathbf{Q}] = [R:A][A:\mathbf{Q}] = \infty$. ■

§ 1.2 Splitting Fields

This section is about answering the question of the existence of a field extension of the field of coefficients of a polynomial that contains all the roots of the polynomial.

We will start this section with a very important theorem which is due to Kronecker.

Theorem (Kronecker Theorem)

Let F be a field, let $f(x)$ be a nonzero polynomial over F , then there exist an extension field E of the field F and $c \in E$ such that $f(c) = 0$.

Proof:

Let F be a field, $f(x)$ be a non-constant polynomial in $F[x]$, since $F[x]$ is unique factorization domain, then $f(x) = p(x)f_1(x)f_2(x)\dots f_n(x)$, where $p(x), f_i(x)$ are irreducible polynomial over F , for all $i=1,2,\dots,n$

Now finding an extension field E for F for which $p(x)$ has a root in E will be sufficient to prove the theorem.

since $p(x)$ is irreducible polynomial in $F[x]$, then $(p(x))$ is a maximal ideal of $F[x]$ and hence $F[x]/(p(x))$ is a field. Now consider the natural homomorphism $s: F \rightarrow F[x]/(p(x))$ by $s(a) = a + (p(x))$, for $a \in F$.

the kernel of s is $\ker s = \{a \in F : s(a) = (p(x))\}$, now $s(a) = (p(x))$ implies $a + (p(x)) = (p(x))$, then $a - 0 = a \in (p(x))$ hence $p(x) \mid a$, but $\deg p(x) > 0$, then a must be zero, hence $\ker s = \{0\}$ and so s is monomorphism map (of course we can show this directly because any nontrivial homomorphism between any two fields are monomorphism)

Now $F \cong s(F) = \{a + (p(x)) : a \in F\} \subseteq F[x]/(p(x)) = E$

so we find a field extension $E \mid F$ by the means of this map s and now we have to show that E will contain a zero for $p(x)$.

so consider the evaluation homomorphism $\phi_c : F[x] \rightarrow F[x]/(p(x))$ by letting $c = x + (p(x))$, where $\phi_c(a) = a$ for $a \in F$ and $\phi_c(x) = c = x + (p(x))$.

now if $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_i \in F$, for all $i=0,1,2,\dots,n$

$$\begin{aligned} \phi_c(p(x)) &= \phi_c(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) \\ &= a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0 \\ &= a_n (x + (p(x)))^n + a_{n-1} (x + (p(x)))^{n-1} + \dots + a_1 (x + (p(x))) + a_0 \end{aligned}$$

$$=(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) + (p(x))$$

$$=p(x)+(p(x))=(p(x))=0 \text{ in } \frac{F[x]}{(p(x))}$$

hence we found an element c in E such that $p(c)=0$, therefore $f(c)=0$. ■

Example

Let $F=\mathbf{R}$, let $p(x)=x^2+1$, which irreducible polynomial over \mathbf{R} and has no root in \mathbf{R} , let $c = x+(p(x)) = x+(x^2+1)$, $E = \frac{\mathbf{R}[x]}{(x^2+1)}$ so $p(c) = c^2+1 = (x+(x^2+1))^2+1 = x^2+1+(x^2+1) = (x^2+1) = 0$ in E . ◀

Corollary

If $p(x)$ is an irreducible polynomial over a field F , then there exist an extension field $E | F$ where $p(x)$ has a root in E and $[E:F] = \deg p(x)$.

Proof:

Let $p(x) \in F[x]$ with $\deg p(x) > 0$, by kronecker theorem there is an extension field $E | F$ and $c \in E$ such that $p(c) = 0$.

Now consider $F[c]$ will be same as $F(c)$ because c is algebraic and that $E = F(c)$ because of the effect of the evaluation homomorphism. Hence $[F(c):F] = \deg p(x)$ and therefore $[E:F] = \deg p(x)$.

Example

Back to the previous example, $\mathbf{C} = \mathbf{R}(c) = \{a+bc : a, b \in \mathbf{R}\}$, hence we may think of c as i and that will give algebraic construction to the complex numbers. ◀

Theorem

Let F be a field, let $f(x) \in F[x]$ be a non-constant polynomial, then $f(x)$ has at most n roots in any extension field $E | F$.

Proof:

Let F be field and $f(x) \in F[x]$, $\deg f(x) = n \geq 1$, the proof will be by induction on n .

So let $P(n)$ be the proposition that $f(x) \in F[x]$ be a non-constant polynomial, then $f(x)$ have at most n roots in any extension field $E | F$.

-Basis step: $P(1)$

let $\deg f(x) = 1$, then $f(x) = ax+b$, $a \neq 0, b \in F$, so in any extension field $E | F$, if $c \in E$ such that $f(c) = 0$, then $c = -a^{-1}b$, hence $f(x)$ has only one root $c \in F$ and thus $P(1)$ is true.

-Induction step : $P(1) \wedge P(2) \wedge \dots \wedge P(k-1) \rightarrow P(k)$
 assume $P(i)$ is true for all $i=1,2,3,\dots,k-1$ i.e. the result in any field for all polynomial of degree less than k , let $\deg f(x)=k$ and $E | F$ is an extension field, so we have two cases :

case 1 : if E has no root for $f(x)$, then we are done.

case 2 : if E contains a root for $f(x)$ i.e. there exist $c \in E$ such that $f(c)=0$, so suppose $f(x)=(x-c)^m q(x)$, $q(c) \neq 0$ and $m \leq n$.

Now $q(x) \in E[x]$ and $\deg q(x)=n-m$,

assume $b \neq c \in E$ such that $f(b)=0$, then $(b-c)^m q(b) = 0$, hence $q(b) = 0$ i.e. b is a root for $q(x)$ over E and by induction hypothesis $q(x)$ has at most $n-m$ roots in E , which together with m roots for c shows that $f(x)$ has at most n roots in E . ■

Examples

(1) Consider $f(x) = x^2 + 1 \in \mathbf{R}[x]$ has two roots in $\mathbf{C} | \mathbf{R}$ ($\pm i \in \mathbf{C}$).

(2) let $f(x) = x^2 - 3 \in \mathbf{Q}[x]$ has two roots in $\mathbf{Q}(\sqrt{3})$. ◀

Remark

Even when we are proving this theorem we didn't realize the importance of the commutative axiom of the field e.g. in any division ring which fails to be a field only because of the commutative axiom doesn't hold it doesn't follow the result of the theorem for instance take $f(x) = x^2 + 1$ in the ring of quaternion, then $f(x)$ has three roots i, j, k .

even with a commutative non-integral domain ($ab=0$ while $a \neq 0, b \neq 0$) the theorem will not follow, for instance take $f(x) = ax$, then $f(x)=0$ either $x=0$ or $x=b$.

Corollary

If $f(x) \in F[x]$, $\deg f(x) = n \geq 1$, then there exist a finite extension field $E | F$, where $f(x)$ has a root and $[E:F] \leq n$.

Proof:

Let $p(x)$ be an irreducible polynomial factor of $f(x)$, any root of $p(x)$ will be a root for $f(x)$, hence $[E:F] = \deg p(x) \leq n$, where E is a simple extension field of F generated by the root of $p(x)$. ■

Definition

Let F be a field, A polynomial $f(x) \in F[x]$ is said to split over a field $E \supseteq F$, if $f(x)$ can be factored as a product of linear factor in $E[x]$.

Examples

(1) Let $f(x) = x^2 + 1 \in \mathbf{R}[x]$, then $f(x) = (x - i)(x + i)$ in $\mathbf{C}[x]$, hence $f(x)$ splits over \mathbf{C} , but note that $f(x) = x^2 + 1 \in \mathbf{Q}[x]$ splits over $\mathbf{Q}(i)$ and \mathbf{C} , by the previous corollary $[\mathbf{Q}(i):\mathbf{Q}] = 2 \leq 2 = \deg f(x)$.

(2) consider $f(x) = (x^2 - 3)(x^2 - 2) \in \mathbf{Q}[x]$ which is split over $\mathbf{Q}(\sqrt{3}, \sqrt{2})$ and it doesn't split over $\mathbf{Q}(\sqrt{2})$ because $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$ and by the previous corollary $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}] = 2 \leq 4 = \deg(f(x))$. ◀

Theorem

Let F be a field, $f(x) \in F[x]$ with $\deg f(x) = n \geq 1$, then there is an extension $E | F$ of degree at most $n!$ in which $f(x)$ has n roots.

Proof:

Let F be field, with $\deg f(x) = n \geq 1$, the proof will be by the induction on n .

-Basis step: if $n=1$, then $E=F$ and $[E:F] = 1 \leq 1!$.

- Induction step :

suppose the result is true for all polynomial of degree less than n ,

suppose $f(x)$ has a root c in extension field $E_0 | F$, then by the previous corollary,

$[E_0:F] \leq n$, also $f(x) = (x-c)q(x)$, where $q(x) \in E_0[x]$, $q(x)$ has degree $n-1$ so by the induction hypothesis there is an extension field $E | E_0$ with $[E:E_0] \leq (n-1)!$

which $q(x)$ has all $n-1$ roots there, so now $f(x)$ has n roots in E and by the

degree equation : $[E:F] = [E:E_0][E_0:F] \leq n(n-1)! \leq n!$. ■

This theorem leads us to believe that given any polynomial $f(x) \in F[x]$, where F is a field, then there exist an extension field $E | F$ where $f(x)$ has $n = \deg f(x)$ roots or there exist an extension field E of F such that $f(x)$ factors completely into linear factors and this lead us to define a new type of field extensions $E | F$ where a polynomial $f(x)$ splits up completely over E as a product of linear factors.

Definition

Let F be a field, $f(x) \in F[x]$ and $E | F$ is a field extension, the E is said to be the splitting field for $f(x)$ over F if :

1- $f(x)$ splits over E .

2- there is no proper intermediate field L of $E | F$ where $f(x)$ splits over L .

Examples

(1) the field C is the splitting field for $f(x) = x^2 + 1$ over R because $f(x) = (x - i)(x + i)$ over $C[x]$, and if L is an intermediate field between C and R which $f(x) = x^2 + 1$ split over L , then by the degree equation $2 = [C:R] = [C:L][L:R]$, which implies that either $L = R$ or $L = C$, hence there is no proper intermediate field.

(2) The field C is not the splitting field for $x^2 + 1$ over Q , because $x^2 + 1$ split over $Q(i)$ and $Q \subset Q(i) \subset C$.

in part (1) and (2) we notice that $[C:R] = 2 = 2!$ and $[Q(i):Q] = 2! = \deg f(x)$.

(3) the splitting field for $f(x) = (x^2 - 2)(x^2 - 3)$ is the field $Q(\sqrt{2}, \sqrt{3})$ over Q , since $\pm \sqrt{2}, \pm \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$, and $[Q(\sqrt{3}, \sqrt{2}):Q] = 4 \leq 4! = \deg f(x)$.

(4) Consider $f(x) = x^3 - 2 \in Q[x]$, then the splitting field for this polynomial is not just $Q(\sqrt[3]{2})$, because $f(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}(\frac{-1 + i\sqrt{3}}{2}))(x + \sqrt[3]{2}(\frac{-1 - i\sqrt{3}}{2}))$ and the other complex roots are not in $Q(\sqrt[3]{2})$.

Now to find the splitting field E , one can suggest adjoining the complex roots to $Q(\sqrt[3]{2})$, and then $f(x)$ will split over E but we may notice that any field containing $i\sqrt{3}$ and $(\sqrt[3]{2})$ will contain the three roots of $f(x)$, hence we can take $E = Q(i\sqrt{3}, \sqrt[3]{2})$ to be the splitting field for $f(x) =$ over Q .

$[E:Q] = [E: Q(\sqrt[3]{2})][Q(\sqrt[3]{2}):Q] = 6 = (\deg f(x))!$

(5) now we apply the same technique we just apply it for part (4) for the polynomial $f(x) = x^4 + 4 \in Q[x]$, then

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

$$f(x) = (x - i + 1)(x + i + 1)(x - 1 + i)(x - 1 - i)$$

so the roots of this polynomial are in $Q(i)$, hence $Q(i)$ is the splitting field for $f(x)$ over Q and $[Q(i):Q] \leq 4! = \deg f(x)$.

(6) Consider $f(x) = x^n - 1 \in \mathbf{Q}[x]$, $n \geq 1$, then to find the roots for $f(x)$ we use some theorems from complex analysis which states that $x^n - 1 = 0$ has a zero of the form $re^{i\theta}$, then $r^n e^{ni\theta} = 1$, then $r=1$ and $ni\theta = 2\pi k$, $k=0,1,2,\dots,n-1$, and hence $\theta = \frac{2\pi k}{n}$, $k=0,1,\dots,n-1$.

So the splitting field for $f(x)$ is the field generated by these numbers which we will study them in details in section 3.1 cyclotomic field.

(7) Let $f(x) = x^2 + [1] \in Z_2[x]$, $f(x)=0$, then $x^2 + [1]=0$, then $x=[1],[3] \in Z_4$ hence the splitting field for $f(x)$ is Z_4 over Z_2 . ◀

Theorem

Let F be a field and $f(x)$ be a polynomial in $F[x]$ of degree n , let $E | F$ be a field extension, then if $f(x) = a(x - c_1)(x - c_2)\dots(x - c_n)$ in $E[x]$, then $F(c_1, c_2, \dots, c_n)$ is a splitting field for $f(x)$ over F .

Proof:

Let F be a field and $f(x)$ be a polynomial in $F[x]$ of degree n , let $E | F$ be a field extension.

Suppose $f(x) = a(x - c_1)(x - c_2)\dots(x - c_n)$ in $E[x]$, then $f(x)$ has n roots in E and so $f(x)$ split over $F(c_1, c_2, \dots, c_n)$.

Now suppose L be an intermediate field of $F(c_1, c_2, \dots, c_n) | F$ such that $f(x)$ splits also over L ,

since $F[x]$ is a UFD, then $f(x) = a(x - c_1)(x - c_2)\dots(x - c_n)$ in $L[x]$ and that implies c_1, c_2, \dots, c_n in L , then $F(c_1, c_2, \dots, c_n) \subseteq L$ and so $F(c_1, c_2, \dots, c_n)$ is the smallest intermediate field over which $f(x)$ splits. ■

Now we move to a very important question:

Given $f(x) \in F[x]$, $n = \deg f(x) \geq 1$, is there an extension field E of F for which $f(x)$ split?

And if there is such an extension field is it unique ?

The answer for this question will be in the next few theorems.

Theorem

Let F be a field, $f(x) \in F[x]$, $n = \deg f(x) \geq 1$, then there exist a splitting field for $f(x)$ over F .

Proof:

Let F be a field, $f(x) \in F[x]$, $n = \deg f(x) \geq 1$, the proof will be by the induction on n .

-Basis step: $n=1$

Let $\deg f(x)=1$, then $f(x)=ax+b$, $a \neq 0, b \in F$, then F is the splitting field for $f(x)=ax+b$ over F , hence the theorem true when $n=1$.

- Induction step:

assume the result hold for all polynomials with a degree less than $k-1$, assume $f(x) \in F[x]$, $\deg f(x)=k$, then by kronecker theorem's, there exist an extension field E_1 of F and $c_1 \in E_1$, such that $f(c_1)=0$, then

$f(x)=(x-c_1)q(x)$ in $E_1[x]$, degree of $q(x) = k-1$, hence by the induction hypothesis $q(x)$ split over E_1 , let us say $q(x)=a(x-c_2)(x-c_3)\dots(x-c_k)$ in $E_1[x]$, hence

$f(x)=a(x-c_1)(x-c_2)\dots(x-c_n)$ in $E_1[x]$, therefore by the previous theorem $F(c_1, c_2, \dots, c_n)$ is the splitting field for $f(x)$ over F . ■

Definition

Let $E|F$ be algebraic field extension, two elements a and $b \in E$ are said to be conjugate over F if $\text{irr}(a, F) = \text{irr}(b, F)$.

Examples

(1) In $\mathbf{C}|\mathbf{R}$, $i, -i$ are conjugate over \mathbf{R} because $\text{irr}(i, \mathbf{R}) = x^2 + 1 = \text{irr}(-i, \mathbf{R})$.

(2) In $\mathbf{Q}(\sqrt{3})|\mathbf{Q}$, $\sqrt{3}, -\sqrt{3}$ are conjugate over \mathbf{Q} since $\text{irr}(\sqrt{3}, \mathbf{Q}) = x^2 - 3 = \text{irr}(-\sqrt{3}, \mathbf{Q})$.

(3) the concept of conjugate elements in the complex number is the same here for the case of $\mathbf{C}|\mathbf{R}$, if $a, b \in \mathbf{R}$, $b \neq 0$ then the conjugate of $a+bi$ is $a-bi$ because $\text{irr}(a+bi, \mathbf{R}) = x^2 - 2abx + a^2 + b^2 = \text{irr}(a-bi, \mathbf{R})$. ◀

Theorem (The Conjugation Theorem)

Let F be a field and let a and b be algebraic element over F with $\deg(a, F) = n$, the map $\psi : F(a) \rightarrow F(b)$ defined by :

$$\psi(c_{n-1}a^{n-1} + \dots + c_1a + c_0) = c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \dots + c_1b + c_0$$

for $a_0, a_1, \dots, a_{n-1} \in F$ is an isomorphism of $F(a)$ onto $F(b)$ if and only if a and b are conjugate.

Proof:

Let F be a field and a, b are algebraic over F .
 assume ψ be an isomorphism of $F(a)$ onto $F(b)$, then let
 $\text{irr}(a, F) = c_0 + c_1x + \dots + c_nx^n$, then $c_0 + c_1a + \dots + c_na^n = 0$ and so
 $\psi(c_0 + c_1a + \dots + c_na^n) = c_nb^n + c_{n-1}b^{n-1} + \dots + c_1b + c_0 = 0$.
 So $\text{irr}(b, F) \mid \text{irr}(a, F)$, by the same way for ψ^{-1} to get that $\text{irr}(a, F) \mid \text{irr}(b, F)$ and
 hence
 $\text{irr}(a, F) = \text{irr}(b, F)$ and therefore a and b are conjugate over F .

conversely, suppose $p(x) = \text{irr}(a, F) = \text{irr}(b, F)$, then $\ker \phi_a = \ker \phi_b = (p(x))$
 where $\phi_a : F[x] \rightarrow F(a)$
 now since a and b are algebraic over F , then we have
 $\psi_a : F[x]/(p(x)) \rightarrow F(a)$ and $\psi_b : F[x]/(p(x)) \rightarrow F(b)$ are isomorphism maps, let
 $\psi = \psi_b \psi_a^{-1}$, then ψ is isomorphism map.

Now let

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \dots + c_1a + c_0 \in F(a), \text{ then}$$

$$\psi_b \psi_a^{-1}(c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \dots + c_1a + c_0) = \psi_b((c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1x + c_0) + (p(x)))$$

$$= c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \dots + c_1b + c_0 \quad \blacksquare$$

Corollary

Let $f(x) \in \mathbf{R}[x]$, if $f(a+bi) = 0$ for $a+bi \in \mathbf{C}$, then $f(a-bi) = 0$
 i.e. complex zeros of polynomials with real coefficients occur in conjugate pairs.

Proof:

Since $\text{irr}(i, \mathbf{R}) = \text{irr}(-i, \mathbf{R}) = x^2 + 1$, then $i, -i$ are conjugate over \mathbf{R} , so by the conjugation theorem $\psi : \mathbf{R}(i) \rightarrow \mathbf{R}(-i)$ which is $\psi : \mathbf{C} \rightarrow \mathbf{C}$, and $\psi(a+bi) = a-bi$ which is isomorphism, thus
 $f(a+bi) = c_n(a+bi)^n + c_{n-1}(a+bi)^{n-1} + \dots + c_1(a+bi) + c_0 = 0$ where
 $c_n, c_{n-1}, \dots, c_0 \in \mathbf{R}$
 $\psi(f(a+bi)) = 0 \rightarrow c_n(a-bi)^n + c_{n-1}(a-bi)^{n-1} + \dots + c_1(a-bi) + c_0 = 0$
 So $f(a-bi) = 0$. ■

Example

The polynomial $f(x) = (x-1)(x^2 + 1)$ has one real root 1 and two complex conjugate roots $i, -i$. ◀

Note:

Let $E|F$ be an algebraic field extension, then the relation \approx on E define by for all $a, b \in E$, $a \approx b$ if and only if a and b are conjugate.

is an equivalence relation:

1- Reflexive : $a \approx a$

since $\text{irr}(a, F) = \text{irr}(a, F)$, then a and a are conjugate over F .

2- Symmetric: for all $a, b \in E$, $a \approx b \rightarrow b \approx a$.

assume $a \approx b$, then $\text{irr}(a, F) = \text{irr}(b, F)$, therefore $\text{irr}(b, F) = \text{irr}(a, F)$, hence $b \approx a$.

3- Transitive: for all a, b and $c \in E$, $a \approx b$ and $b \approx c \rightarrow a \approx c$.

assume $a \approx b$ and $b \approx c$, then $\text{irr}(a, F) = \text{irr}(b, F) = \text{irr}(c, F)$ and thus $a \approx c$.

Theorem

Let σ be an isomorphism from the field F onto the field F' , let

$f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$ and $g(y) = \sigma(a_0) + \sigma(a_1)y + \dots + \sigma(a_n)y^n \in F'$.

If E is the splitting field for $f(x)$ over F and E' is the splitting field for $g(y)$ over F' , then $E \cong E'$.

Proof:

The proof will be by the induction on $n = \deg f(x)$,

-Basis step: $n=1$, then $E=F$ and $E'=F'$ and therefore $E \cong E'$.

- Induction step: suppose the result hold for all polynomials of degree less than n , let c be a root for $f(x)$ over F , then $f(x) = (x-c)q(x)$ in $F(c)[x]$.

let c' be a root for $g(x)$ over F' , then $g(x) = (x-c')q'(x)$ in $F'(c')[x]$.

where $\deg f(x)$ and $\deg g(x) = n-1$ and by σ we have :

$F[x] \cong F'[x]$ And that imply $\frac{F[x]}{(p(x))} \cong \frac{F[x]}{(p_1(x))}$ where $p(x)$ and $p_1(x)$ are

irreducible factor for $f(x)$, $g(x)$, $p(c)=0$ and $p_1(c)=0$,

then we have $F(c) \cong F'(c')$. (by conjugation theorem)

Now since E is the splitting field for $f(x)$ over F , it is also the splitting field for $q(x)$ over $F(c)$ i.e. all roots of $q(x)$ are in E and if E wasn't a splitting field for $q(x)$ over $F(c)$ and L is such a field, then because L will contain $F(c)$, then all the roots will be in L which is contradict the minimality of E as a splitting field for $f(x)$ over $F(c)$. (similarly E' is splitting field for $q_1(x)$ over $F'(c')$).

and now by the induction hypothesis we have $F(c) \cong F'(c')$ and then $E \cong E'$. ■

Now all our work to show the uniqueness of a splitting field for a polynomial over a field is come in the next corollary.

Corollary (Uniqueness of the Splitting Field)

Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

Proof:

In the previous theorem, Take to be σ the identity mapping from F to itself and E and E' to be the splitting fields for $f(x)$ over F where $g(x)=f(x)$. ■

Now after this corollary we can write:

“ E is the splitting field for $f(x)$ over F ”

In fact to show the uniqueness it took from too much work to collect all the material in this section which i tool it from many sources and I collected together and present it here in this way, I hope you like the work for this result.

§1.3 Separable Extensions

Consider $f(x) = (x-1)^2 \in \mathbf{Q}[x]$, then $f(x)$ has one root in the splitting field \mathbf{Q} for $f(x)$ over \mathbf{Q} , and we notice that this root is repeated root twice, this will lead us for the following Definition

Definition

If $f(x)$ is a polynomial over F and c is a root for $f(x)$ in some field extension $E | F$, then the multiplicity of c is the greatest positive integer m such that $(x-c)^m | f(x)$ over E , we said that $f(x)$ has a multiplicity root of c if $m > 1$.
i.e. if c is a root for $f(x) \in f[x]$ of multiplicity m , then $f(x) = (x-c)^m g(x)$ in $E[x]$ and $g(c) \neq 0$.

Examples

(1) let $\mathbf{C} | \mathbf{R}$, $f(x) = x^2 + 1$, then the root $i, -i$ are of multiplicity one.

(2) In $\mathbf{R} | \mathbf{R}$, $f(x) = x^3 + 3x^2 + 3x + 1 = (x+1)^3$, the multiplicity of -1 is 3. ◀

Now we will give a definition to the derivation of polynomial in any given field, this concept is similar to what we already know in calculus and the properties is also similar and we will just list them without proof.

Definition

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in f[x]$, then the derivative of $f(x)$ written as $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1 \in f[x]$.

Properties: for any $f(x), g(x) \in f[x]$, and any $c \in F$,

- 1- $(f(x) + g(x))' = f'(x) + g'(x)$
- 2- $(cf(x))' = cf'(x)$
- 3- $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Examples

(1) $f(x) = x^2 - 2 \in \mathbf{Q}[x]$, then $f'(x) = 2x \in \mathbf{Q}[x]$ and $f(x)$ has no multiple root in $\mathbf{Q}(\sqrt{2})[x]$.

(2) $f(x) = x^3 - 6x^2 + 12x - 8 \in \mathbf{Q}[x]$, $f'(x) = 3x^2 - 12x + 12 \in \mathbf{Q}[x]$. Also note $f(x)$ has multiple root $c = 2$ over \mathbf{Q} , and $f'(2) = 0$.

(3) let F be a field with $\text{Char}(F)=p$, then if $f(x) = x^p \in F[x]$, then

$$f'(x) = px^{p-1} = 0 \text{ over } F.$$

Thus the result from the calculus that a polynomial whose derivative is 0 must be constant is not longer needed to be true. ◀

Definition

An irreducible polynomial over F is separable if it has no multiple roots (i.e. all root are distinct [of multiplicity one]). A polynomial which is not separable is inseparable and any polynomial $f(x)$ in $F[x]$ is separable if all its irreducible polynomial factors in $F[x]$ are separable, otherwise $f(x)$ is inseparable.

Note:

Here we are talking about $f(x)$ being separable in its splitting field over F .

Example

$f(x) = x^2 - 3$ is separable over \mathbf{Q} , since $\pm\sqrt{3}$ are distinct root over $\mathbf{Q}(\sqrt{3})$ which is the splitting field for $f(x)$ over F , however $f(x) = (x^2 - 3)^n, n \geq 2$ is inseparable since it has multiple roots $\pm\sqrt{3}$ each with multiplicity n . ◀

Theorem

Let F be a field and $0 \neq f(x) \in F[x]$, let c be a root of $f(x)$ in some extension field $E | F$, then c is a multiple root if and only if $f'(c) = 0$.

Proof:

Let F be a field, $0 \neq f(x) \in F[x]$, $c \in E$ is a root of $f(x)$ in $E | F$.

Suppose c is a multiple root, let c be of multiplicity $m > 1$, then

$$f(x) = (x - c)^m g(x) \text{ in } E[x] \text{ and } g(c) \neq 0. f'(x) = m(x - c)^{m-1} g(x) + (x - c)^m g'(x) \text{ in } E[x] f'(c) = 0.$$

Conversely, suppose $f'(c) = 0$, then $\deg(f(x)) \geq 2$, by division algorithm in $F[x]$ (Euclidean domain), then $f(x) = (x - c)^2 q(x) + r(x)$, $r(x) = 0$ or $\deg(r(x)) < 2$

$$f'(x) = 2(x - c)q(x) + (x - c)^2 q'(x) + r'(x)$$

$f'(c) = 0$ implies $r'(c) = 0$, but $\deg(r(x)) < 2$, if $\deg r(x)=0$, then $f(c)=r(c)=0$ implies $r(x) \equiv 0$ if $\deg r(x)=1$, then $r(x) = a_1x + b_1$, $a_1 \neq 0, b_1 \in E$. $r'(x) = a_1 \neq 0$, but $r'(c) = 0$ contradiction.

Therefore, $f(x) = (x - c)^2 q(x)$, hence c is multiple root of $f(x)$. ■

Example

In $\mathbf{C} | \mathbf{R}$, $f(x) = (x^2 + i)^2$, then i is multiple root of multiplicity = 2,
 $f'(x) = 2(x^2 + i)(2x) \rightarrow f'(i) = 0$. ◀

Theorem
 let F be a field, an irreducible polynomial $p(x)$ over F is separable if and only if $p(x)$ and $p'(x)$ are relatively prime i.e. $\gcd(p(x), p'(x)) \in F - \{0\}$.

Proof:

Let F be a field, let $p(x) \in F[x]$ be irreducible polynomial suppose $f(x)$ is separable, let c be a root for $f(x)$ in some extension field $E | F$, then

$$p(x) = (x - c)q(x) \text{ in } F(c)[x], q(c) \neq 0.$$

$$p'(x) = (x - c)q'(x) + q(x).$$

$$p'(c) = q(c) \neq 0.$$

Let $d(x) = \gcd(p(x), p'(x))$, then $d(c) \neq 0$, because if c is a root for $p(x)$ and $p'(x)$, then it will be a root for $d(x)$ and by the same thing for all the roots c_1, c_2, \dots, c_k of $f(x)$ none of them will be root for $p'(x)$, hence none of them is root for $d(x)$, hence $d(x)$ is unit, $d(x)=1$.
 and so $p(x)$ and $p'(x)$ relatively prime.

Conversely, suppose $d(x) = a$, $a \in F - \{0\}$, let c be a root for $p(x)$ over F with a multiplicity of m , then $p(x) = (x - c)^m q(x)$ in $F(c)[x]$, $q(c) \neq 0 \Rightarrow (x - c)^m | p(x)$
 $p'(x) = m(x - c)^{m-1} q(x) + (x - c)^m q'(x) = (x - c)^{m-1} \{mq(x) + (x - c)q'(x)\} \Rightarrow (x - c)^{m-1} | p'(x)$
 and hence $(x - c)^{m-1} | \gcd(p(x), p'(x)) \rightarrow (x - c)^{m-1} | a$, therefore $m = 1$, hence every root for $p(x)$ is of multiplicity = 1, hence $p(x)$ is separable. ■

Theorem
 Let F be a field, $p(x) \in F[x]$, and let $p(x)$ be an irreducible polynomial in $F[x]$, then $p(x)$ is separable if and only if $p'(x) \neq 0$.

Proof:

Let F be a field, $p(x)$ is irreducible polynomial in $F[x]$ suppose $p(x)$ is separable and $p'(x) = 0$, then $\gcd(p(x), p'(x)) = p(x)$

Hence $p(x) = d(x) \neq 1$, contradiction of the previous theorem where $p(x)$ is separable, so $d(x)=1$, therefore $p'(x) \neq 0$.

Conversely, assume $p'(x) \neq 0$, since $p(x)$ is irreducible polynomial the only divisors of $p(x)$ are $p(x)$ and 1 in $F[x]$, so the only common divisors of $p(x)$ and $p'(x)$ are 1 and $p(x)$, since $1 \leq \deg p'(x) < \deg p(x)$, 1 is the only common divisor of $p'(x)$ and $p(x)$, hence $d(x)=1$, therefore $p(x)$ is separable. ■

Examples

(1) To show that $f(x) = (x^2 - 3)(x^2 - 2)$ is separable, let $p_1(x) = x^2 - 2$ and $p_2(x) = x^2 - 3$, then $p_1'(x) = p_2'(x) = 2x \neq 0$, hence $p_1'(x)$ and $p_2'(x)$ are separable hence $f(x) = (x^2 - 3)(x^2 - 2)$ is separable.

(2) $f(x) = x^{p^n} - x$ over Z_p , $f'(x) = p^n x^{p^n-1} - [1] = [-1] \neq [0]$, therefore is separable.

(3) Consider $f(x) = x^n - 1$, $f(x) \in F[x]$

Case I: if $\text{char}(F) = 0$ or $\text{char}(F)$ does not divide n , then $f'(x) = nx^{n-1} = 0$ if and only if $x = 0$ which is not root for $f(x)$, hence $\gcd(f(x), f'(x)) = 1$, therefore $f(x)$ is separable.

Case II: $\text{char}(F)=p \mid n$, then $f'(x) = nx^{n-1} = n(px^{n/p-1}) \equiv 0$ and so $f(x)$ is inseparable (every root of $f(x)$ is multiple). ◀

Corollary

If $p(x) \in F[x]$ is irreducible, then

i) if $\text{char}(F)=0$, $p(x)$ has no multiple root ($p(x)$ is separable)

ii) if $\text{char}(F)=p$ (p is prime), then $f(x)$ has a multiple root only if it is of the form $p(x)=q(x^p)$, $q(x^p) \in F[x^p]$.

Proof:

Let $p(x) \in F[x]$ is irreducible polynomial.

i) Suppose F is a field and $\text{char}(F)=0$, let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$p'(x) = na_n x^{n-1} + \dots + ia_i x^{i-1} + \dots + a_1$, since $\text{char}(F)=0$ then there exist $i > 0$, such that $a_i \neq 0$, therefore $ia_i \neq 0$ $p'(x) \neq 0$, hence $p(x)$ is separable.

ii) Suppose F is a field, $\text{char}(F) = p > 0$, let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, and suppose $f(x)$ has a multiple root, then $p'(x) = n a_n x^{n-1} + \dots + a_1 = 0$, then
 $p(x) = a'_m x^{mp} + a'_{m-1} x^{(m-1)p} + \dots + a'_1 x^p + a'_0$ (transform it)
 $p_1(x) = a'_m x^m + a'_{m-1} x^{(m-1)} + \dots + a'_1 x + a'_0 \in F[x^p]$, hence
 $p(x) = q(x^p) \in F[x^p]$. ■

Definition

1) Let $E | F$ be an extension field and $c \in E$ be an algebraic element over F , then c is called separable over F if $\text{irr}(c, F)$ is separable. Otherwise c is called inseparable.

2) If $E | F$ is an algebraic extension field, then $F | E$ is called separable if every element of E is separable over F otherwise $E | F$ is called inseparable.

Examples

(1) In $\mathbb{Q}(\sqrt{3}) | \mathbb{Q}$, the element $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ is separable because
 $p(x) = \text{irr}(\sqrt{3}, \mathbb{Q}) = x^2 + 3$, $p'(x) = 2x \neq 0$, hence $p(x)$ is separable.

(2) In $\mathbb{Z}_3 | \mathbb{Z}_2$, the element $[2] \in \mathbb{Z}_3$ is separable because
 $p(x) = \text{irr}([2], \mathbb{Z}_2) = x^2 - 1$, $p'(x) = 2x \rightarrow p'([2]) = [4] = [1] \neq [0]$, hence $p(x)$ is separable.

(3) Any field F with $\text{char}(F) = 0$ and algebraic extension $E | F$ is separable since by the previous corollary, every irreducible polynomial is separable. ◀

Before we go further, we will give some theorems that will help us in our work.

Theorem

Let F be a field of characteristic $p > 0$, let $\sigma : F \rightarrow F$ defined by $F(a) = a^p$, for all $a \in F$ then σ is an isomorphism map.

Proof:

Let $a, b \in F$, then

$$\begin{aligned}\sigma(a+b) &= (a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k \\ &= a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-1} a b^{p-1} + b^p\end{aligned}$$

Since $p \mid \binom{p}{i}$, $\forall i = 1, 2, \dots, p-1$, then

$$(a+b)^p = a^p + b^p, \text{ since } \text{char}(F) = p.$$

$$\text{So } \sigma(a+b) = \sigma(a) + \sigma(b)$$

$$\text{Let } \sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$$

Therefore, σ is a homomorphism map from F onto F , thus σ is monomorphism map.

Now $\sigma[F] = \{\sigma(a) : a \in F\} = \{a^p : a \in F\}$, hence $\sigma : F \rightarrow \sigma[F] \leq F$ is an isomorphism map. ■

Definition

- 1) The image of the monomorphism in the previous theorem is denoted by $F^p = \{a^p : a \in F\} \leq F$.
- 2) The isomorphism $\sigma : F \rightarrow F^p$ is called Frobenius isomorphism.

Definition

A field F with $\text{char}(F) = p > 0$ is called perfect if $F = F^p$, any field of $\text{char}(F) = 0$ is also called perfect.

Examples

(1) Every finite field F is perfect.

indeed Consider the Frobenius isomorphism $\sigma : F \rightarrow F^p$, then

$|F| = |\sigma(F)| = |F^p|$, hence $|F^p| = |F|$ and since $F^p \subseteq F$, therefore $F = F^p$, hence F is perfect.

(2) Z_2 is perfect. ◀

CHAPTER 2

The Fundamental Theorem of Galois Theory

In this chapter we will study the major theorem in this project which is the theorem hold the project title “The fundamental theorem of Galois” which is due to the young french mathematician Galois who proved this theorem with a help of what he found from the work done by Abel, so we will start this chapter by defining the fixed field and Galois group and Galois extension and then we will present the fundamental theorem of Galois with a lot of examples to show its beauty.

§ 2.1 Automorphisms and Fixed Fields

In this section we will study the relationship between an automorphism map of a field E and the elements of E by observing the effect of such automorphism σ on a subfield F of E .

Definition

An automorphism $\sigma \in \text{Aut}(E)$ is said to fix an element $c \in E$ if $\sigma(c) = c$, given F is a subfield (or a subset) of E , then an automorphism σ is said to fix F if it fixes all the elements of F i.e. $\sigma(a) = a$, for all $a \in F$.

Notation

Given $E | F$ a field extension, the set of all automorphism of E that is fix F is denoted by $G(E | F)$ i.e. $\sigma \in G(E | F)$, then $\sigma(a) = a$ for all $a \in F$.

Examples

(1) Given any field E , let 1 be the identity automorphism of E then 1 fixes F for any subfield F of E .

(2) Let $E = \mathbb{Q}(\sqrt{3})$, then the map $\sigma : E \rightarrow E$ defined by

$\sigma(a + b\sqrt{3}) = (a - b\sqrt{3})$, for $a, b \in \mathbb{Q}$, then σ is an automorphism because

$$\begin{aligned} \text{i) } \sigma(a + b\sqrt{3} + c + d\sqrt{3}) &= \sigma(a + c + (b + d)\sqrt{3}) = (a + c) - (b + d)\sqrt{3} = a - b\sqrt{3} + c - d\sqrt{3} \\ &= \sigma(a + b\sqrt{3}) + \sigma(c + d\sqrt{3}) \end{aligned}$$

$$\begin{aligned} \text{ii) } \sigma((a + b\sqrt{3})(c + d\sqrt{3})) &= \sigma(ac + (ad + cb)\sqrt{3} + 3bd) = ac + 3bd - (ad + cb)\sqrt{3} \\ &= a(c - d\sqrt{3}) - b\sqrt{3}(c - d\sqrt{3}) = (a - b\sqrt{3})(c - d\sqrt{3}) \\ &= \sigma(a + b\sqrt{3})\sigma(c + d\sqrt{3}). \end{aligned}$$

hence σ is homomorphism.

iii) $\ker \sigma = \{a + b\sqrt{3} : \sigma(a + b\sqrt{3}) = 0\}$, $\sigma(a + b\sqrt{3}) = 0$, then $a - b\sqrt{3} = 0$ and hence $a = b = 0$

and so $\ker \sigma = \{0\}$, therefore σ is monomorphism.

$$\text{iv) } \sigma(E) = \{\sigma(a + b\sqrt{3}) : a + b\sqrt{3} \in E\} = \{a - b\sqrt{3} : a, b \in \mathbb{Q}\} = E = \mathbb{Q}(\sqrt{3})$$

hence σ is an automorphism, also note that $\sigma = \psi : \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{Q}(-\sqrt{3})$ (the conjugation map).

Now let $a \in \mathbb{Q}$, then $\sigma(a) = a$, hence σ fixes \mathbb{Q} and so $H = \{1, \sigma\}$ subgroup of $\text{Aut}(E)$ which fixes \mathbb{Q} and as we will see later $H = G(\mathbb{Q}(\sqrt{3}) | \mathbb{Q})$. ◀

Theorem

Let $E | F$ be a field extension, then $G(E | F)$ is a subgroup of $\text{Aut}(E)$ and is called the group of automorphism of E relative to F .

Proof:

Since $\mathbf{1}$ fixes F , then $\mathbf{1} \in G(E | F)$, hence $G(E | F) \neq \phi$, now let $\sigma, \pi \in G(E | F)$, let $a \in F$, then $\sigma\pi^{-1}(a) = \sigma(a) = a$, hence $\sigma\pi^{-1}$ fixes F , therefore $\sigma\pi^{-1} \in G(E | F)$, therefore $G(E | F) \leq \text{Aut}(E)$. ■

Definition

Let G be a group of automorphisms of the field E , we denote E_G as the set of all $a \in E$ such that a is fixed by every element in G .

$$E_G = \{a \in E : \sigma(a) = a, \forall \sigma \in G\}.$$

Theorem

Let G be a group of automorphisms of the field E , then E_G is a subfield of E , called the fixed field of E for G . furthermore if $E | F$ is a field extension, then $E_{G(E|F)}$ is an intermediate field of $E | F$.

Proof:

since $0, 1 \in E_G$, then $E_G \neq \phi$,

let $a, b \in E_G$ and $\sigma \in G$, then

i) $\sigma(a-b) = \sigma(a) - \sigma(b) = a-b$, hence $a-b \in E_G$.

ii) $\sigma(ab^{-1}) = \sigma(a) \sigma(b^{-1}) = ab^{-1}$, $ab^{-1} \in E_G$, therefore E_G is a subfield of E

Now if $E | F$ is a field extension, then it clear that $F \subseteq E_{G(E|F)} \subseteq E$. ■

Example

Consider $E = \mathbf{Q}(\sqrt{3})$, $G = \{\mathbf{1}, \psi\}$, then we have:

$$\psi(a + b\sqrt{3}) = a - b\sqrt{3} = a + b\sqrt{3}, \text{ then } b=0, \text{ hence } E_G = \mathbf{Q}.$$
 ◀

The next theorem is very useful in determining the automorphisms of an algebraic field extension.

Theorem

Let $E|F$ be a field extension and let $c \in E$ be an algebraic element over F , then for any $\sigma \in G(E|F)$ we have $\sigma(c)$ is a root for $\text{irr}(c,F)$ i.e. $G(E|F)$ permutes the roots of the irreducible polynomial of c .

Proof:

Let $E|F$ be a field extension, let $c \in E$ be algebraic over F and $p(x) = \text{irr}(c,F) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, $a_i \in F, i = 0, 1, 2, \dots, n-1$, then

$p(c) = 0$ i.e. $c^n + a_{n-1}c^{n-1} + \dots + a_1c + a_0 = 0$, so

$\sigma(c^n + a_{n-1}c^{n-1} + \dots + a_1c + a_0) = \sigma(0)$, then

$(\sigma(c))^n + a_{n-1}(\sigma(c))^{n-1} + \dots + a_1\sigma(c) + a_0 = 0$, and so $\sigma(c)$ is a root for $p(x)$. ■

now we will take advantage of this theorem to show the beautiful duality between the field extension and a subgroup of the group of automorphism.

Examples

(1) Consider $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$, let $E = \mathbb{Q}(\sqrt{3})$

a) we want to find $G(E|\mathbb{Q})$

so let $\sigma \in G(E|\mathbb{Q})$ i.e. σ fixes \mathbb{Q} , now because $\sqrt{3}$ is algebraic over \mathbb{Q} then

$\sigma(\sqrt{3})$ will be zero for $\text{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$, so the two possibilities for $\sigma(\sqrt{3})$

are the two roots of $x^2 - 3$, so either $\sigma(\sqrt{3}) = \sqrt{3}$ or $\sigma(\sqrt{3}) = -\sqrt{3}$

if $\sigma(\sqrt{3}) = \sqrt{3}$, then for $a + b\sqrt{3} \in E$, we have

$\sigma(a + b\sqrt{3}) = a + b\sigma(\sqrt{3}) = a + b\sqrt{3}$, hence $\sigma = 1$

if $\sigma(\sqrt{3}) = -\sqrt{3}$, then for $a + b\sqrt{3} \in E$, we have

$\sigma(a + b\sqrt{3}) = a - b\sigma(\sqrt{3}) = a - b\sqrt{3}$

hence $G(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) = \{1, \sigma\}$ which is cyclic group of order 2 and we can notice that $|G(\mathbb{Q}(\sqrt{3})|\mathbb{Q})| = [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$.

b) now assume that we have $G(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) = \{1, \sigma\}$ as described above and we want to find $\mathbb{Q}(\sqrt{3})_{G(\mathbb{Q}(\sqrt{3})|\mathbb{Q})} = K$.

let $c = a + b\sqrt{3} \in K$, then $\sigma(c) = \sigma(a + b\sqrt{3}) = a + b\sqrt{3}$, then $a - b\sqrt{3} = a + b\sqrt{3}$, hence $b = 0$ and that means $c = a \in \mathbb{Q}$ which show $\mathbb{Q}(\sqrt{3})_{G(\mathbb{Q}(\sqrt{3})|\mathbb{Q})} = \mathbb{Q}(\sqrt{3})_{\{1, \sigma\}} = \mathbb{Q}$.

(2) Consider $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$, as before let $\sigma \in G(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$, then σ is completely

determined by the action on $\sqrt[3]{2}$, let $c = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$, then

$\sigma(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\sigma(\sqrt[3]{2}) + c(\sigma(\sqrt[3]{2}))^2$, since $\sigma(\sqrt[3]{2})$ is a root for

$x^3 - 2 = 0$ and the only real root for $\text{irr}(\sqrt[3]{2}, \mathbb{Q})$ is $\sqrt[3]{2}$, then $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ and

hence we will get $\sigma(c)=c$ for all $c \in \mathbf{Q}(\sqrt[3]{2})$, therefore $\sigma=1$ and $G(\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q})=\{1\}$ and $|G(\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q})|=1<[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}]=3$.

Now assume we find $\mathbf{Q}(\sqrt[3]{2})_{\{1\}}$, so let $c \in \mathbf{Q}(\sqrt[3]{2})_{\{1\}}$, then $1(c)=\sigma(c)=c$ and so every element of $\mathbf{Q}(\sqrt[3]{2})$ is fixed by σ , therefore $\mathbf{Q}(\sqrt[3]{2})_{\{1\}}=\mathbf{Q}(\sqrt[3]{2})$.

in example (1) and (2), we can notice that if E is generated over F by some collection of elements, then any automorphism $\sigma \in G(E|F)$ is completely determined by what it does to the generators.

(3) Consider $E=\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $F=\mathbf{Q}$,

a) we want to find $G(E|F)$, so let $\sigma \in G(E|F)$ and we are going to study it's action in the generators $\sqrt{3}, \sqrt{2}$, so we have 4 possibilities:

$\sigma_1(\sqrt{2})=\sqrt{2}$	$\sigma_2(\sqrt{2})=-\sqrt{2}$
$\sigma_1(\sqrt{3})=\sqrt{3}$	$\sigma_2(\sqrt{3})=\sqrt{3}$
$\sigma_3(\sqrt{2})=\sqrt{2}$	$\sigma_4(\sqrt{2})=-\sqrt{2}$
$\sigma_3(\sqrt{3})=-\sqrt{3}$	$\sigma_4(\sqrt{3})=-\sqrt{3}$

since E is the splitting field for $(x^2 - 2)(x^3 - 3)$ over F.

Now σ_1 is the trivial automorphism **1**.

let σ represent σ_2 .

and π represent σ_3 .

and we want to find a σ_4 such that $\{1, \sigma, \pi, \sigma_4\}$ is a group,

let $w=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \in E$

so $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$

$\pi(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=1+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$

note that $\sigma^2(\sqrt{2})=\sqrt{2}$ and $\pi^2(\sqrt{3})=\sqrt{3}$, hence $\sigma^2, \pi^2 = 1$

compute $\sigma\pi$, then $\sigma\pi(\sqrt{2})=\sigma(\pi(\sqrt{2}))=\sigma(\sqrt{2})=-\sqrt{2}$

$\sigma\pi(\sqrt{3})=\sigma(\pi(\sqrt{3}))=\sigma(-\sqrt{3})=-\sqrt{3}$

So $\sigma_4=\sigma\pi$, so we have $\{1, \sigma, \pi, \sigma\pi\}$ and this is isomorphic to the klein 4 group or we can verify that this is indeed group by checking the group axioms.

b) Now for $E=\mathbf{Q}(\sqrt{2}, \sqrt{3})$ we want to find the following fixed fields :

$E_{\{1\}}, E_{\{1,\sigma\}}, E_{\{1,\sigma\pi\}}, E_{\{1,\pi\}}, E_{\{1,\sigma,\pi,\sigma\pi\}}$

so for $\{1, \sigma\pi\}$, let $w=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \in E$

$\sigma\pi(w)=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, then $b=c=0$ and therefore

$E_{\{1,\sigma\pi\}}=\mathbf{Q}(\sqrt{6})$ and so on.

we will find :

Subgroup of $G(E F)$	Fixed field
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\pi\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \pi\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma\pi\sigma\pi\}$	\mathbb{Q}

(4) Determine the automorphism of the extension $E = \mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}(\sqrt{2})$ explicitly.

since we have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$, then $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = \frac{[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]} = \frac{4}{2} = 2$

and since $\{1, 2^{\frac{1}{4}}, 2^{\frac{2}{4}}, 2^{\frac{3}{4}}\}$ is a basis for $\mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}$ and $\{1, \sqrt{2}\}$ is a basis for

$\mathbb{Q}(\sqrt{2}) | \mathbb{Q}$, then $\{1, 2^{\frac{1}{4}}\}$ is a basis for $\mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}(\sqrt{2})$.

Now let $p(x) = \text{irr}(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})) = x^2 + Ax + B \in \mathbb{Q}(\sqrt{2})$, then

$$(\sqrt[4]{2})^2 + (a+b\sqrt{2})\sqrt[4]{2} + c+d\sqrt{2} = 0, a, b, c \text{ and } d \in \mathbb{Q}, \text{ then}$$

$$(1+d)\sqrt{2} + a\sqrt[4]{2} + b\sqrt[4]{8} + c = 0, \text{ then } d = -1 \text{ and } a = b = c = 0$$

$$\text{therefore } \text{irr}(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})) = x^2 - \sqrt{2}$$

now if $\sigma \in G(\mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}(\sqrt{2}))$, then either $\sigma = 1$ or $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$, hence

$$G(\mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}(\sqrt{2})) = \{1, \sigma\}. \quad \blacktriangleleft$$

Theorem

Let E be a field and $\sigma_1, \sigma_2, \dots, \sigma_n$ are distinct automorphisms of E , then $\forall a \in E, \forall a_1, a_2, \dots, a_n \in E$, if $a_1\sigma_1(a) + a_2\sigma_2(a) + \dots + a_n\sigma_n(a) = 0$ then $a_1 = a_2 = \dots = a_n = 0$.

Proof:

proof by the induction on n .

-basis step : $n=1$, then $a_1\sigma_1(a) = 0$, for all $a \in E$, then $a_1 = 0$ since $\sigma_1(a) \neq 0, a \neq 0$

-Induction step : assume the theorem is valid for all $1 \leq k \leq n$.

Suppose

$$a_1\sigma_1(a) + a_2\sigma_2(a) + \dots + a_n\sigma_n(a) = 0 \text{ for all } a \in E \quad (*)$$

and suppose some a_1, a_2, \dots, a_n are not zero say $a_i \neq 0, 1 \leq i \leq n$, since $\sigma_1, \sigma_2, \dots, \sigma_n$ are distinct automorphism, then there exist $b \in E$ such that $\sigma_i(a) \neq \sigma(a)$, since (*) is valid for $ab \in E$ also, then

$$a_1 \sigma_1(ab) + a_2 \sigma_2(ab) + \dots + a_n \sigma_n(ab) = 0$$

$$a_1 \sigma_1(a) \sigma_1(b) + a_2 \sigma_2(a) \sigma_2(b) + \dots + a_n \sigma_n(a) \sigma_n(b) = 0, \text{ multiplying (*) by } \sigma_n(b)$$

and subtracting yield :

$$a_1 (\sigma_n(b) - \sigma_1(b)) \sigma_1(a) + a_2 (\sigma_n(b) - \sigma_2(b)) \sigma_2(a) + \dots + a_{n-1} (\sigma_n(b) - \sigma_{n-1}(b)) \sigma_{n-1}(a) = 0$$

for all $a \in E$ and since $a_i (\sigma_n(b) - \sigma_i(b)) \neq 0$, which is contradiction with the induction hypothesis, hence the theorem is true for all positive integers. ■

Theorem

Let H be a finite set of automorphism of the field E , then:

- i) $|H| \leq [E: E_H]$
- ii) $|H| = [E: E_H]$ if H is a group.

Proof:

(i) suppose not i.e. $|H| > [E: E_H]$, then let $[E: E_H] = n < \infty$ let b_1, b_2, \dots, b_n be a basis for $E | E_H$, there exist $n+1$ distinct automorphism

$\sigma_1, \sigma_2, \dots, \sigma_{n+1} \in G(E | E_H)$, then the system :

$$\sigma_1(b_1)x_1 + \sigma_2(b_1)x_2 + \dots + \sigma_{n+1}(b_1)x_{n+1} = 0$$

$$\sigma_1(b_2)x_1 + \sigma_2(b_2)x_2 + \dots + \sigma_{n+1}(b_2)x_{n+1} = 0$$

.

.

.

$$\sigma_1(b_n)x_1 + \sigma_2(b_n)x_2 + \dots + \sigma_{n+1}(b_n)x_{n+1} = 0$$

will has a nontrivial solution $x_1 = a_1, x_2 = a_2, \dots, x_{n+1} = a_{n+1}$ in E .

thus

$$\sigma_1(b_i)a_1 + \sigma_2(b_i)a_2 + \dots + \sigma_{n+1}(b_i)a_{n+1} = 0, \text{ for all } i=1,2,\dots,n$$

and for every $a \in E, a = \sum_{i=1}^n k_i b_i, k_i \in E_H$ and so $\sigma_j(a) = \sigma_j(\sum_{i=1}^n k_i b_i) = \sum_{i=1}^n k_i \sigma_j(b_i)$

since $c_i \in E_H$ and so

$$a_1 \sigma_1(a) + a_2 \sigma_2(a) + \dots + a_{n+1} \sigma_{n+1}(a) = 0$$

$$a_1 \sum_{i=1}^n k_i \sigma_1(b_i) + a_2 \sum_{i=1}^n k_i \sigma_2(b_i) + \dots + a_{n+1} \sum_{i=1}^n k_i \sigma_{n+1}(b_i) = 0$$

$$\sum_{i=1}^n k_i (a_1 \sigma_1(b_i) + \dots + a_{n+1} \sigma_{n+1}(b_i)) = 0, \text{ for all } a \in E, \text{ however this contradict the}$$

previous theorem, therefore $|H| \leq [E: E_H]$.

ii) By (ii), $|H| \leq [E : E_H]$, we have to show the equality hold for H being a group, assume $n = |H| < [E : E_H]$, then there exist $n + 1$ linearly independent elements of E over E_H say b_1, b_2, \dots, b_{n+1} , so the system of n homogeneous linear equations in the $n + 1$ unknowns x_1, x_2, \dots, x_{n+1} , then

$$\begin{bmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_{n+1}) \\ \sigma_2(b_1) & \sigma_2(b_2) & \cdots & \sigma_2(b_{n+1}) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(b_1) & \sigma_n(b_2) & \cdots & \sigma_n(b_{n+1}) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$x_1 \sigma_i(b_1) + x_2 \sigma_i(b_2) + \dots + x_{n+1} \sigma_i(b_{n+1}) = 0, \quad i = 1, 2, \dots, n$$

Has nontrivial solution $X = (x_1, x_2, \dots, x_n) = (a_1, a_2, \dots, a_n)$ and $\exists a_i$ such that $a_i \neq 0$ and $a_i \notin E_H$, otherwise contradict with ???.

Now we will choose X to be the solution of the smallest numbers of nonzero members say m.

$m = 1$, then $a_1 \sigma_1(b_1) = 0$, then a_1 is zero

So assume $m > 1$, reordering X we have

$$\begin{bmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_m) \\ \sigma_2(b_1) & \sigma_2(b_2) & \cdots & \sigma_2(b_m) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(b_1) & \sigma_n(b_2) & \cdots & \sigma_n(b_m) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad a_j \neq 0, \quad \forall j = 1, 2, \dots, m$$

$$x_1 \sigma_i(b_1) + x_2 \sigma_i(b_2) + \dots + x_m \sigma_i(b_m) = 0, \quad i = 1, 2, \dots, n \quad (*)$$

Let $\sigma_1 = 1$, the identity map, then

$a_1 b_1 + \dots + a_m b_m = 0 \rightarrow$ multiply by a_m^{-1} to make the coefficient of $b_m = 1$, then if all $a_1, a_2, \dots, a_m \in E_H$, then say $a_1 \notin E_H$ (one from the above), and hence for some $\sigma_j, \sigma_j(a_1) \neq a_1$

So apply σ_j to (*), then

$$\sigma_j(a_1 \sigma_i(b_1)) + \dots + \sigma_j(a_m \sigma_i(b_m)) = 0, \quad i = 1, 2, \dots, n$$

$$\sigma_j(a_1) \sigma_{ij}(b_1) + \dots + \sigma_j(a_m) \sigma_{ij}(b_m) = 0, \quad i = 1, 2, \dots, n \quad (**)$$

Where $\sigma_{ij} = \sigma_i \circ \sigma_j$, now since $H = \{\sigma_{1j}, \sigma_{2j}, \dots, \sigma_{nj}\} = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ in some arrangement.

So subtract (**) from (*)

$$(a_1 - \sigma_j(a_1))(\sigma_i(b_1)) + \dots + (a_{m-1} - \sigma_j(a_{m-1}))(\sigma_i(b_{m-1})) = 0, \quad i = 1, 2, \dots, n$$

And since $a_1 - \sigma_j(a_1) \neq 0$, then this a solution for the previous matrix system

having fewer than m nonzero this contradiction, hence $[E : E_H] > |H|$ is false,

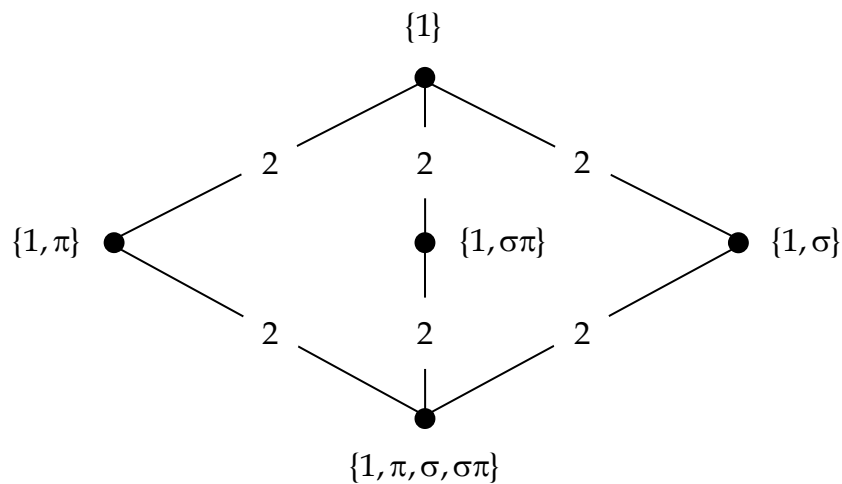
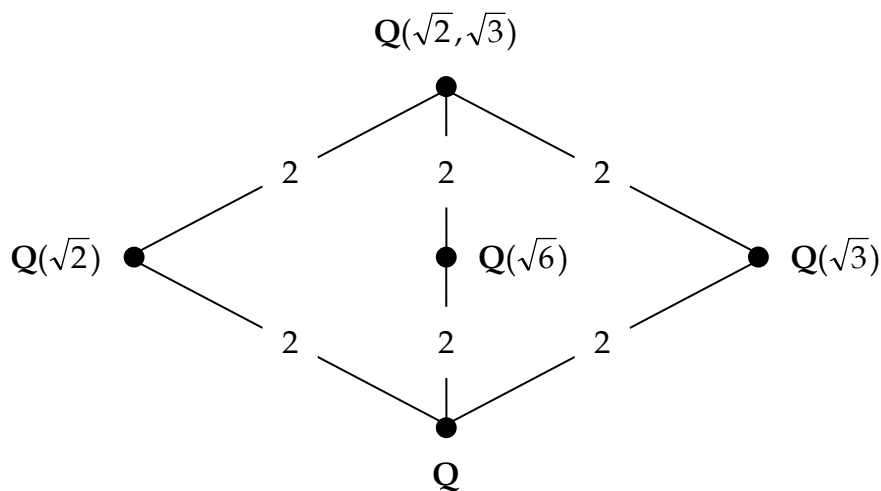
hence $[E : E_H] = |H|$ ■

Examples

(1) In the previous example about $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$, $H = G(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) = \{1, \sigma\}$, which is a cyclic group of order 2, hence $H = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt{3})_H] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$.

(2) In $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$, $H = G(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = \{1\}$ which is the trivial group, hence $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})_H] = 1 = |H|$.

(3) In $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$, to find $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{6})] = |\{1, \sigma\pi}| = 2$, the following diagram can be useful: ◀



Theorem

Let H be finite group of automorphisms of the field E , then $H = G(E | E_H)$.

Proof:

It is clear that $H \subseteq G(E|E_H)$, now $G(E|E_H)$ is finite group, by the previous theorem $|G(E : E_H)| = [E : E_{G(E|E_H)}]$ now we need to show that $E = E_{G(E|E_H)}$, so let $a \in E_H$, then for all $\sigma \in G(E|E_H)$, $\sigma(a) = a$, so $a \in E_{G(E|E_H)}$ hence $E_H \subseteq E_{G(E|E_H)}$ and by the same way pick $a \in E_{G(E|E_H)}$, then all $\sigma \in G(E|E_H)$, $\sigma(a) = a$, since $H \subseteq G(E|E_H)$, then $\sigma(a) = a$ for all $\sigma \in H$, hence $a \in E_H$, therefore $E_{G(E|E_H)} \subseteq E_H$ and that implies $E_H = E_{G(E|E_H)}$ now $|G(E : E_H)| = [E : E_{G(E|E_H)}] = [E : E_H] = |H|$ and since $H \subseteq G(E|E_H)$ and $G(E|E_H)$ is a finite, then $H = G(E|E_H)$. ■

Example

In $\mathbf{Q}(\sqrt{2}, \sqrt{3})|\mathbf{Q}$, $H = \{1, \sigma\}$, then $F_H = \mathbf{Q}(\sqrt{6})$
 $G(F|F_H) = H$.

As we see the example about $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$, we get that if $E = \mathbf{Q}(\sqrt[3]{2})$, then we have $\mathbf{Q} \neq E_{G(E|\mathbf{Q})}$ ◀

§ 2.2: The Fundamental Theorem of Galois Theory

In this section we desire to have $E | F$ such that $F = E_{G(E|F)}$

i.e. the fixed field by the group of automorphisms that fix F is just F itself (nothing less, nothing more) so we need some sort of condition on $E | F$ to force $F = E_{G(E|F)}$ and we wish to generalize this to any intermediate field of $E | F$ so that $L = E_{G(E|L)}$, where $F \subseteq L \subseteq E$.

Definition

Let $E | F$ be a finite field extension, if $F = E_{G(E|F)}$ then $G(E | F)$ is called the Galois group of $E | F$ and $E | F$ is called a Galois extension.

Remark

1- if $\sigma \in G(E | F)$, the Galois group of $E | F$, then σ must move all elements of E except the elements of F .

2- from the definition and the previous theorems

$$|G(E | F)| = [E : E_{G(E|F)}] = [E : F] \quad (*)$$

Example

Let us go back to our 3 Examples

(1) $\mathbb{Q}(\sqrt{3}) | \mathbb{Q}$ is Galois extension because $G = G(\mathbb{Q}(\sqrt{3}) | \mathbb{Q}) = \{1, \sigma\}$,

$\mathbb{Q}(\sqrt{3})_G = \mathbb{Q}$, hence $G(\mathbb{Q}(\sqrt{3}) | \mathbb{Q})$ is the Galois group of $\mathbb{Q}(\sqrt{3}) | \mathbb{Q}$.

We already know that $\mathbb{Q}(\sqrt{3}) | \mathbb{Q}$ is separable ($\text{char}(\mathbb{Q}(\sqrt{3})) = 0$) and $\mathbb{Q}(\sqrt{3})$ is the splitting field of $\text{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$ over \mathbb{Q} .

(2) $\mathbb{Q}(\sqrt[3]{2}) | \mathbb{Q}$ is not a Galois extension because $G(\mathbb{Q}(\sqrt[3]{2}) | \mathbb{Q}) = \{1\}$, hence

$\mathbb{Q}(\sqrt[3]{2})_{\{1\}} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$ notice $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of

$\text{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ over \mathbb{Q} .

(3) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F = \mathbb{Q}$, then $E | F$ is Galois extension and $G(E | F)$ is the Galois group of $E | F$, because $E_{G(E|F)} = E_{\{1, \pi, \sigma, \sigma\pi\}} = F$.

We already know that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is separable ($\text{char}(E) = 0$) and E is the splitting field of $(x^2 - 2)(x^3 - 3)$ over \mathbb{Q} . ◀

Now we will present a very important theorem in determining whether $E | F$ is a Galois extension or not.

Theorem

Let $E|F$ be a finite field extension, then the following conditions are equivalent:

- i) $E|F$ is a Galois extension.
- ii) $E|F$ is separable and E is the splitting field for a separable polynomial in $F[x]$.

Proof:

Suppose $[E:F]=n$, let $H \leq G(E|F)$, then $|H| = [E:E_H] \leq [E:F]=n$.

(i) \rightarrow (ii)

Suppose $G(E|F)$ be the Galois group of $E|F$, then $|G(E|F)| = [E:F]=n$, since $E|F$ is a finite field extension, then $E|F$ is an algebraic field extension and hence it is generated by some element in E over F i.e. $E=F(c_1, c_2, \dots, c_n)$ for some $c_i \in E, i = 1, 2, \dots, n$.

Let $G(E|F) = \{1 = \sigma_1, \sigma_2, \dots, \sigma_n\}$ and let $a \in E$, consider the set $\{\sigma_i(a) : i = 1, 2, \dots, n\}$ which is nonempty set because $\sigma_1(a) = a$ is there.

Now let $a = a_1, a_2, \dots, a_m$ be m distinct elements of this set and

$$a_i = \sigma_i(a), i = 1, 2, \dots, n$$

$$\sigma_j(a_i) = \sigma_j(\sigma_i(a)) = \sigma_j \sigma_i(a) = \sigma_r(a) = a_r, \quad 1 \leq r \leq m.$$

Now for all $1 \leq k \leq n$, the set $\sigma_k(a_1), \sigma_k(a_2), \dots, \sigma_k(a_m)$ are distinct elements. let $f_a(x) = (x - a_1)(x - a_2) \dots (x - a_m)$, then all the roots of $f_a(x)$ are distinct and lies in F , Now for any $\pi \in G(E|F)$ will permute the roots a_1, a_2, \dots, a_m , hence $f_a(x)$ has coefficients which are fixed by all the elements of $G(E|F)$, hence $f_a(x) \in F[x]$.

since $F = E_{G(E|F)}$, then $a = a_1$ is a root for a separable polynomial $f_a(x) \in F[x]$ and $f_a(x)$ splits over E , so in general for any c_i , $1 \leq i \leq n$, c_i is a root of a separable polynomial $f_{c_i}(x) \in F[x]$ and $f_{c_i}(x)$ splits over E , thus all roots of $f(x) = f_{c_1}(x) f_{c_2}(x) \dots f_{c_n}(x) \in F[x]$ are in E .

Since $E = F(c_1, c_2, \dots, c_n)$ and c_i is a root for $f(x)$, then E is the splitting field for $f(x)$ over F and that $f(x)$ is separable which we will get $E|F$ is separable.

(ii) \rightarrow (i)

Suppose E is the splitting field of a separable polynomial $f(x)$ over F , let m be the number of distinct roots of $f(x)$ in E but not in F the proof of the result will be by induction on m .

- Basis step: $m=0$.

assume $m=0$, then the splitting field for $f(x)$ over F is F itself and hence $G(F|F) = \{1\}$, hence $F = E_{G(F|F)}$ and also $[F:F]=1 = |G(F|F)|$, hence the result is true when $m=0$.

-Induction step:

Let the result hold for all field extension $S | T$ such that S is the splitting field for a separable polynomial $g(x) \in T[x]$ with $g(x)$ having fewer than $m \geq 1$ roots outside T . (this the induction hypothesis)

Now let $f(x) = p_1(x)p_2(x)\dots p_k(x)$, where each $p_i(x)$ is irreducible and separable in $F[x]$, since $m \geq 1$, $\deg p_i(x) > 1$ for some i .

without loss of generality let us assume $i=1$ i.e. $\deg p_1(x) = t > 1$ and let $a \in E$ such a root, then $[F(a):F] = t$ and $p_1(x)$ has t distinct root $a = a_1, a_2, \dots, a_t$ because it is separable, so by the conjugation theorem, there exist $\psi_1, \psi_2, \dots, \psi_t$ such that

$\psi_i : F(a) \rightarrow F(a_i)$ and this can be extended to an automorphism σ_i of E because E is the splitting field for $f(x)$ over both $F(a)$ and $F(a_i)$ and we have σ_i fixes F .

Now suppose $c \in E_{G(E|F)}$, since $f(x)$ has fewer than m roots outside $F(a)$, then by the induction hypothesis $F(a) = E_{G(E|F(a))}$ and $G(E | F(a)) \leq G(E | F)$ and

$E_{G(E|F)} \subseteq E_{G(E|F(a))} = F(a)$, now $c \in E_{G(E|F)} = F(a)$, then $c = c_0 + c_1 a + \dots + c_{t-1} a^{t-1}$, $c_i \in F, i=0,1,2,\dots,t-1$

$\sigma_i(c) = c = c_0 + c_1 a_i + \dots + c_{t-1} a_i^{t-1}$, construct the following polynomial :

$g(x) = (c_0 - c) + c_1 x + \dots + c_{t-1} x^{t-1}$ and this will have $a = a_1, a_2, \dots, a_t$ as a roots ,

therefore it has t distinct roots and its degree less than t , hence $g(x) \equiv 0$ and so $c_0 - c = 0$ and so $c = c_0 \in F$, hence $F = E_{G(E|F)}$ and therefore $G(E | F)$ is the Galois group of $E | F$. ■

Examples

(1) Consider $f(x) = x^3 - 2$ over \mathbf{Q} .

To find its splitting field over \mathbf{Q} , then we will factor $f(x)$ as

$f(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}(\frac{-1 + \sqrt{-3}}{2}))(x - \sqrt[3]{2}(\frac{-1 - \sqrt{-3}}{2}))$ and so the roots of $f(x)$ are

$\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$, where $\rho = \frac{-1 + \sqrt{-3}}{2}$, hence we can take the splitting field for

$f(x)$ over \mathbf{Q} is $E = \mathbf{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2})$ which is isomorphic to $\mathbf{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2})$.

So $|G(E | F)| = [E:\mathbf{Q}] = [E:\mathbf{Q}(\sqrt[3]{2})][\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}] = 2 \cdot 3 = 6$

And $G(E | F)$ is the Galois group of $E = \mathbf{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2})$.

To find the element of $G(E | F)$ let $\sigma \in G(E | F)$, then it will map $\sqrt[3]{2}, \rho\sqrt[3]{2}$ to $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$, so we will have 6 possibilities and that we have 6 automorphisms.

$\sigma_1(\sqrt[3]{2}) = \rho \sqrt[3]{2}$ $\sigma_1(\rho) = \rho$	$\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}$ $\sigma_2(\rho) = \rho^2 = -\rho - 1$
$\sigma_3(\sqrt[3]{2}) = \sqrt[3]{2}$ $\sigma_3(\rho) = \rho$	$\sigma_4(\sqrt[3]{2}) = \rho^2 \sqrt[3]{2}$ $\sigma_4(\rho) = \rho$
$\sigma_5(\sqrt[3]{2}) = \rho^2 \sqrt[3]{2}$ $\sigma_5(\rho) = \rho^2$	$\sigma_6(\sqrt[3]{2}) = \rho \sqrt[3]{2}$ $\sigma_6(\rho) = \rho^2$

So as we did before let $\sigma = \sigma_1, \pi = \sigma_2$

Since the basis of $E = \mathbf{Q}(\sqrt[3]{2}, \rho)$ is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho \sqrt[3]{2}, (\rho \sqrt[3]{2})^2\}$

So

$$\sigma(a + b \sqrt[3]{2} + c(\sqrt[3]{2})^2 + d\rho + e\rho \sqrt[3]{2} + f\rho(\sqrt[3]{2})^2)$$

$$= a + b \sqrt[3]{2} + c(\sqrt[3]{2})^2 + d\rho + e\rho \sqrt[3]{2} + f\rho(\sqrt[3]{2})^2$$

and so on

now :

$$1- \sigma^2(\sqrt[3]{2}) = \sigma(\rho \sqrt[3]{2}) = \rho \rho \sqrt[3]{2} = \rho^2 \sqrt[3]{2}.$$

$$\sigma^2(\rho) = \sigma(\sigma(\rho)) = \sigma(\rho) = \rho.$$

hence σ^2 represent σ_4

$$2- \pi \sigma^2(\sqrt[3]{2}) = \pi(\rho^2 \sqrt[3]{2}) = \rho^2 \sqrt[3]{2}$$

$$\pi \sigma^2(\rho) = \pi(\rho) = \rho^2$$

hence $\pi \sigma^2$ represent σ_5

$$3- \pi \sigma(\sqrt[3]{2}) = \pi(\rho \sqrt[3]{2}) = \rho^2 \sqrt[3]{2}$$

$$\pi \sigma(\rho) = \pi(\rho) = \rho^2$$

hence $\pi \sigma$ represent σ_6 and we can notice that $\sigma^3 = \pi^2 = 1$

hence $\{1, \sigma, \pi, \pi \sigma^2, \sigma^2, \pi \sigma\}$ is a group of automorphism and that

$$G(\mathbf{Q}(\sqrt[3]{2}, \rho) | \mathbf{Q}) = \langle \sigma, \pi \rangle \cong S_3$$

Subgroup of $G(E F)$	Fixed field
$\langle 1 \rangle$	$\mathbb{Q}(\sqrt[3]{2}, \rho)$
$\langle \sigma \rangle$	$\mathbb{Q}(\rho)$
$\langle \pi \rangle$	$\mathbb{Q}(\sqrt[3]{2})$
$\langle \sigma \pi \rangle$	$\mathbb{Q}(\rho \sqrt[3]{2})$
$\langle \pi \sigma^2 \rangle$	$\mathbb{Q}(\rho^2 \sqrt[3]{2})$
$\langle \sigma, \pi \rangle$	\mathbb{Q}

(2) $\mathbb{Q}(\sqrt[4]{2})$ is not a Galois extension over \mathbb{Q} since every automorphism is send $\sqrt[4]{2}$ to four possible values which they are $\pm \sqrt[4]{2}, \pm i\sqrt[4]{2}$ and only two of them are real and we can notice that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$,

where $\mathbb{Q}(\sqrt{2}) | \mathbb{Q}$ is Galois extension. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

$\mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}(\sqrt{2})$ is Galois extension. $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$

$\mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q}$ is not Galois extension. $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$

Hence this example shows that Galois extension of Galois extension is not necessarily Galois extension. ◀

Theorem: The Fundamental Theorem of Galois Theory

Let $E|F$ be a finite normal and separable field extension, let $G = G(E|F)$, let T be the set of all intermediate fields of $E|F$.

$S(G)$ be the set of all subgroup of G .

then the following properties hold:

(1) $F = E_G$

(2) the mapping $\psi : T \rightarrow S(G)$ defined by $\psi(L) = G(E|L)$, for all $L \in T$ is bijective map and the map $\phi : S(G) \rightarrow T$ defined by $\phi(H) = E_H$ is the inverse of ψ .

Moreover, for all $L \in T$, $[E:L] = |G(E|L)|$ and $[L:F] = [G : G(E|L)]$.

(3) Let $L, L' \in T$, then $L' \subseteq L$ if and only if $G(E|L) \subseteq G(E|L')$

in this case $[L:L'] = [G(E|L') : G(E|L)]$.

(4) Let $L, L' \in T$, $\psi(L) = H$, $\psi(L') = H'$, then there exist $\sigma \in G$ such that $\sigma(L) = L'$ if and only if $\sigma H \sigma^{-1} = H'$.

(5) Let $L \in T$, then $L|F$ is normal extension if and only if $G(E|L)$ is a normal subgroup of G . also $G(L|F) \cong \frac{G(E|F)}{G(E|L)}$.

Proof:

Assume $E|F$ be a finite normal and separable extension.

(1) Since $E|F$ is a finite normal extension (i.e. every irreducible polynomial $f(x) \in F[x]$ such that $f(x)$ has a root in E splits completely into linear factor in $E[x]$), then E is the splitting field for a separable polynomial over F , hence $G(E|L)$ is the Galois group of $E|F$ and therefore $F = E_{G(E|F)}$ i.e. $F = E_G$.

(2) Let $L, L' \in T$, if $L=L'$, then $\psi(L)=G(E|L)=G(E|L')= \psi(L')$ and hence ψ is well defined, suppose $\psi(L)= \psi(L')$, then $G(E|L)=G(E|L')$ and that

$$E_{G(E|L)} = E_{G(E|L')}$$

since $E|F$ is finite, normal and separable extension so by (1),

$L = E_{G(E|L)} = E_{G(E|L')} = L'$, hence ψ is one to one mapping.

Now let $L \in T, H \in S(G)$:

$$\psi \circ \phi(H) = \psi(E_H) = G(E|E_H) = H.$$

$$\phi \circ \psi(L) = \phi(G(E|L)) = E_{G(E|L)} = L \text{ because } E|L \text{ is Galois extension.}$$

hence ϕ is one-to-one mapping and it's the inverse of ψ .

and since $E|L$ is Galois extension, then $[E:L] = |G(E|L)|$,

now $[E:F] = [E:L][L:F]$ (degree equation)

$$|G| = |G(E|L)|[L:F], \text{ then } [L:F] = \frac{|G|}{|G(E|L)|} \text{ and by lagrange's theorem,}$$

$$[L:F] = [G:G(E|L)].$$

(3) Let $L, L' \in T$, assume $L' \subseteq L$ and let $\sigma \in G(E|L)$, then $\sigma(a) = a$ for all $a \in L$, hence $\sigma(a) = a$ for all $a \in L'$, then $\sigma \in G(E|L')$ and so $G(E|L) \subseteq G(E|L')$

now assume $G(E|L) \subseteq G(E|L')$, let $a \in L', \sigma \in G(E|L)$, then $\sigma \in G(E|L')$

$\sigma(a) = a$, where $E|L$ is Galois extension, hence $a \in L$ (because $G(E|L)$ fixes only L)

$$(G(E|L) \subseteq G(E|L'), \text{ then } E_{G(E|L)} = E_{G(E|L')})$$

and therefore $L' \subseteq L$.

Now $[L:L'] = [G(E|L'):G(E|L)]$ (by **(2)** let $E=L, F=L'$)

(4) let $L, L' \in T, \psi(L) = H, \psi(L') = H'$, let $\sigma \in G$

assume $\sigma(L) = L'$, for any $a' \in L'$, there exist $a \in L$, such that $\sigma(a) = a'$, because

σ is an isomorphism from $L \rightarrow L'$, now for all $\pi \in H, \pi(a) = a$, therefore

$\sigma \pi \sigma^{-1}(a') = \sigma \pi(a) = \sigma(a) = a'$, thus $\sigma \pi \sigma^{-1}$ fixes L' , hence $\sigma \pi \sigma^{-1} \in H'$ and so

$$\sigma H \sigma^{-1} \subseteq H',$$

Now $|H'| = [E:L'] = [E:L] = |H| = |\sigma H \sigma^{-1}|$ and since H is finite, then

$$\sigma H \sigma^{-1} = H.$$

conversely, suppose $\sigma H \sigma^{-1} = H$, then for all $a \in L$, for all $\pi \in H$,

$\sigma \pi \sigma^{-1}(\sigma(a)) = \sigma \pi(a) = \sigma(a)$, thus $\sigma(a) \in E_H = L'$, but

$|H| = |H'|$, then $[E:L] = [E:L']$, then $[\sigma(L):F] = [L:F] = [L':F]$, therefore $\sigma(L) = L'$

(or we can say $|\sigma(L)| = |L'|$).

(5) Since $E|F$ is a separable extension, $L|F$ is also a separable extension, then $L|F$ is normal if and only if $L|F$ is a Galois extension equivalently $[L:F] = |G(L|E)|$.

now we will prove that $|G(L|F)| = [L:F]$ if and only if every isomorphism of L fixing F is an automorphism of L fixing F .

1- we will find the number of such isomorphisms.

so let $H = G(E|L)$, $[G:H] = m$ and by (2) $[L:F] = [G:H] = m$, let $\sigma_1 H, \sigma_2 H, \dots, \sigma_m H$ be the m distinct cosets of G with $\sigma_1 H = H$

Now our goal is to show that the element of G in the same coset determines the same isomorphism of L fixing F and vice versa.

for that let $a \in L$, $\pi \in H$, then

$(\sigma_i \circ \pi)(a) = \sigma_i(\pi(a)) = \sigma_i(a)$ for each $i=1,2,\dots,m$ and hence the element in the same coset determines the same isomorphism.

conversely, if $\sigma(a) = \sigma'(a)$, then $a = \sigma^{-1}(\sigma'(a))$ and that $\sigma^{-1}\sigma' \in H$, hence $\sigma H = \sigma' H$ and so σ, σ' determines the same coset.

Therefore the number of distinct isomorphism of L fixing F is $m = [G:H]$.

Now since $|G(L|F)| = m$, any isomorphism of L fixing F is an automorphism of L fixing F .

So $|G(L|F)| = [L:F]$ if and only if every isomorphism of L fixing F is an automorphism of L fixing F if and only if $L|F$ is normal extension.

Now for $\sigma \in G$, σ is an isomorphism of L fixing F , hence σ is an automorphism of L fixing F , hence $\sigma(L) = L$ and by (4) $\sigma(L) = L$ for all $\sigma \in G$ if and only if $\sigma H \sigma^{-1} = H$ i.e. equivalently H is a normal subgroup.

Now let $\varphi: G(L|F) \rightarrow G(E|F)$ defined by $\varphi(\sigma) = \sigma_E$ (where σ_E is σ when restricted to E)

now $\varphi(\sigma\pi) = (\sigma\pi)_E = \sigma_E \pi_E = \varphi(\sigma)\varphi(\pi)$, hence φ is a homomorphism, now for $\varphi(G(L|F)) = G(E|F)$, hence is onto and therefore it is an epimorphism and by

the first isomorphism theorem $G(L|F) \cong \frac{G(E|F)}{\ker \varphi}$

$\ker \varphi = \{\sigma \in G(L|F): \varphi(\sigma) = 1\} = G(E|L)$

hence $G(L|F) \cong \frac{G(E|F)}{G(E|L)}$. ■

Examples

(1) Consider $f(x)=x^4 - 2$ over \mathbf{Q} , then

$f(x) = 0, x^4 - 2 = 0$, then $(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) = 0$, hence the roots of $f(x)$ are $\pm \sqrt[4]{2}, \pm i\sqrt[4]{2}$, let $c = \sqrt[4]{2}$.

now by Eisenstein's criterion $f(x)$ is irreducible over \mathbf{Q} with $p=2$.

also $f(x)$ has all its roots with multiplicity of one, let E be the splitting field for $f(x)$ over \mathbf{Q} , then $E = \mathbf{Q}(\sqrt[4]{2}, i)$ and then $E | \mathbf{Q}$ is normal extension.

now to find a basis for $\mathbf{Q}(c, i)$, by the degree equation:

$$[E:\mathbf{Q}] = [E:\mathbf{Q}(c)][\mathbf{Q}(c):\mathbf{Q}]$$

since $\text{irr}(c, \mathbf{Q}) = f(x)$ and then $\deg(c, \mathbf{Q}) = 4$

$$\text{irr}(i, \mathbf{Q}(c)) = x^2 + 1 \text{ and then } \deg(i, \mathbf{Q}(c)) = 2.$$

$$[E:\mathbf{Q}] = [\mathbf{Q}(c)(i):\mathbf{Q}(c)][\mathbf{Q}(c):\mathbf{Q}] = 2 \cdot 4 = 8.$$

the basis for $\mathbf{Q}(c, i) | \mathbf{Q}(c)$ is $\{1, i\}$ and the basis for $\mathbf{Q}(c) | \mathbf{Q}$ is $\{1, c, c^2, c^3\}$, then

the basis for $\mathbf{Q}(c, i) | \mathbf{Q}$ is $\{1, c, c^2, c^3, ic, ic^2, ic^3, i\}$.

Now by the fundamental theorem of Galois:

$$|G(\mathbf{Q}(c, i) | \mathbf{Q})| = [\mathbf{Q}(c, i):\mathbf{Q}] = 8$$

to determine the elements of the Galois group we do like before.

so assume $\sigma \in G(E | \mathbf{Q})$, then

$\sigma(c)$ will be one of the roots of $x^4 - 2 \in \mathbf{Q}[x]$.

$\sigma(i)$ will be one of the roots of $x^2 + 1 \in \mathbf{Q}(c)[x]$.

hence we have 8 possibilities:

$\sigma_1(\sqrt[4]{2}) = \sqrt[4]{2}$ $\sigma_1(i) = i$	$\sigma_2(\sqrt[4]{2}) = -\sqrt[4]{2}$ $\sigma_2(i) = i$
$\sigma_3(\sqrt[4]{2}) = i\sqrt[4]{2}$ $\sigma_3(i) = i$	$\sigma_4(\sqrt[4]{2}) = -i\sqrt[4]{2}$ $\sigma_4(i) = i$
$\sigma_5(\sqrt[4]{2}) = \sqrt[4]{2}$ $\sigma_5(i) = -i$	$\sigma_6(\sqrt[4]{2}) = -\sqrt[4]{2}$ $\sigma_6(i) = -i$
$\sigma_7(\sqrt[4]{2}) = i\sqrt[4]{2}$ $\sigma_7(i) = -i$	$\sigma_8(\sqrt[4]{2}) = -i\sqrt[4]{2}$ $\sigma_8(i) = -i$

So $G(\mathbf{Q}(c, i) | \mathbf{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_8\}$ which is a non-abelian group of order 8 because

$$\sigma_3\sigma_7(c) = \sigma_3(ic) = \sigma_3(i)\sigma_3(c) = -c$$

$$\sigma_7\sigma_3(c) = \sigma_7(ic) = \sigma_7(i)\sigma_7(c) = c, \text{ hence } \sigma_3\sigma_7 \neq \sigma_7\sigma_3.$$

Now let $L = \mathbf{Q}(c), E = \mathbf{Q}(c, i), F = \mathbf{Q}$, by the fundamental theorem of Galois,

$$\psi(L) = G(E | L) = H$$

$$|G(E | L)| = [E:L] = [\mathbf{Q}(c, i):\mathbf{Q}(c)] = 2$$

so $H = \{1, \sigma\}$, and by checking all the possibilities of σ that is fixes $\mathbf{Q}(c)$ it will be σ_5 and so that $\psi(L) = \{1, \sigma_5\}$ and $\phi(\{1, \sigma_5\}) = L = \mathbf{Q}(c)$, and then we will have the following :

Subgroup of $G(E F)$	Fixed field
$\{1\}$	$E = \mathbf{Q}(c, i)$
$\{1, \sigma_5\}$	$\mathbf{Q}(c)$
$\{1, \sigma_7\}$	$\mathbf{Q}(ic)$
$\{1, \sigma_3\}$	$\mathbf{Q}(c^2, i)$
$\{1, \sigma_6\}$	$\mathbf{Q}(c+ci)$
$\{1, \sigma_8\}$	$\mathbf{Q}(c-ci)$
$\{1, \sigma_3, \sigma_5, \sigma_7\}$	$\mathbf{Q}(c^2)$
$\{1, \sigma_1, \sigma_2, \sigma_3\}$	$\mathbf{Q}(i)$
$\{1, \sigma_3, \sigma_6, \sigma_8\}$	$\mathbf{Q}(ic^2)$
$G(\mathbf{Q}(c, i) \mathbf{Q})$	\mathbf{Q}

(2) Consider $f(x) = x^4 + 1$ over \mathbf{Q} , then the root of $f(x)$ is $x^4 + 1 = 0$, then the root are $\frac{1+i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}$, and $f(x)$ is irreducible over \mathbf{Q} since it is irreducible over \mathbf{Z} ,

let $c = \frac{1+i}{\sqrt{2}}$, one may suggest the splitting field E for $f(x)$ over \mathbf{Q} is

$E = \mathbf{Q}\left(\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}\right)$ but let us take a closer look for E and $c \cdot c = \frac{1+i}{\sqrt{2}}$, then

$$c^2 = \frac{(1+i)(1+i)}{\sqrt{2}\sqrt{2}} = \frac{1+2i-1}{2} = i. \quad c^3 = cc^2 = \frac{-1+i}{\sqrt{2}}.$$

$$c^4 = \frac{(-1+i)(1+i)}{\sqrt{2}\sqrt{2}} = \frac{-1-1}{2} = -1. \quad c^5 = cc^4 = \frac{-1-i}{\sqrt{2}}.$$

$$c^6 = \frac{(-1+i)(-1+i)}{\sqrt{2}\sqrt{2}} = \frac{1-2i-1}{2} = -i. \quad c^7 = cc^6 = \frac{1-i}{\sqrt{2}}.$$

hence we can take $E = \mathbf{Q}(c)$ and $\text{irr}(c, \mathbf{Q}) = f(x)$ with $\text{deg}(c, \mathbf{Q}) = 4$ and so $[E:\mathbf{Q}] = 4$ and the basis for $E | \mathbf{Q}$ will be $\{1, c, c^2, c^3\}$.

By the fundamental theorem of Galois, $[E:\mathbf{Q}] = |G(E|F)| = 4$, now let $\sigma \in G(E|Q)$, then there are only four possibilities for σ which are $\sigma_1(c) = c$, $\sigma_3(c) = c^3$, $\sigma_5(c) = c^5$, $\sigma_7(c) = c^7$

by the same way as we did before we will have the following:

Subgroup of $G(E F)$	Fixed field
$\{1\}$	$E=Q(c)$
$\{1, \sigma_3\}$	$Q(i\sqrt{2})$
$\{1, \sigma_5\}$	$Q(i)$
$\{1, \sigma_7\}$	$Q(\sqrt{2})$
$\{1, \sigma_3, \sigma_5, \sigma_7\}$	Q



CHAPTER 3

Applications

In this chapter we apply the result achieved in the previous chapters to cyclotomic extensions: the splitting field of polynomials $x^n - 1$, $n > 0$. We also consider in this chapter an application of the fundamental theorem of Galois Theory to the case of cubic polynomials.

§ 3.1 Cyclotomic Extensions

In this section we will study the splitting field E for the polynomial $x^n - 1$ over a field F , where $n \geq 1$ and we will study some properties of E .

Definition

Let E be any field and n is a positive integer, let $w \in E$, then w is called the n th root of unity if $w^n = 1$, w is called a primitive n th root of unity if $w^n = 1$ and n is the smallest such positive integer i.e. $w^n = 1$ and $w^m \neq 1$ for all $1 \leq m \leq n$.

Examples

(1) Consider $f(x) = x^3 - 1$ over \mathbf{Q} , then the root of $f(x)$ will be of the form $re^{i\theta}$
So as we know from complex analysis, $r=1$ and $\theta = \frac{2}{3}k\pi$, $k=0,1,2$ and that

$c_k = e^{\frac{2}{3}ki\pi}$ and more specifically $c_0 = 1$, $c_1 = e^{\frac{2}{3}i\pi} = w$, $c_2 = e^{\frac{4}{3}i\pi} = w^2$, hence c_0, c_1, c_2 are 3rd root of unity and also they are primitive 3rd root of unity.

(2) Let $\text{char}(E)=p>0$, let w be an n th root of unity and assume $p \mid n$, then $n=p^k m$, for some positive integers m, k with $\text{gcd}(p, m)=1$, then

$$(w^m - 1)^{p^k} = \sum_{i=0}^{p^k-1} \binom{p^k}{i} (w^m)^{p^k-i} (-1)^i = w^{mp^k} - 1 = w^n - 1 = 0$$

hence $w^m - 1 = 0$, so w also a m th root of unity and thus w is not a primitive n th root of unity.

e.g. let $E=\mathbf{Z}_5$, $p=\text{char}(E)=5$, let $n=10$ and $w=[4]$, then $p \mid n$ ($5 \mid 10$) and also $w^{10} = [4]^{10} \equiv 4^4 4^4 4^2 \pmod{5} \equiv 1 \cdot 1 \cdot 16 \pmod{5} \equiv 1 \pmod{5}$ but $10=5 \cdot 2$ and so $[4]$ is also 2nd root of unity because $[4]^2 \equiv 1 \pmod{5}$. ◀

Definition

The splitting field E of $x^n - 1$ over a field F is called the n th cyclotomic extension of F .

Theorem

Let E be a field, n is positive integer, suppose $\text{char}(E)=p$ which doesn't divide n , let R_n be the set of all n th roots of unity in E , then

- (1) R_n is a cyclic group under field multiplication.
- (2) $|R_n|$ divides n , where $|R_n|$ is the order of R_n .
- (3) if $x^n - 1$ splits into linear factors in $E[x]$, then $|R_n| = n$.

Proof:

Let E be a field with $p = \text{char}(E)$ doesn't divide n ,
 $R_n = \{w \in E : w^n = 1\}$

(1) Since $1^n = 1$, then $1 \in R_n$, hence $R_n \neq \emptyset$.

let $w_1, w_2 \in R_n$, then $(w_1 w_2^{-1})^n = 1$ and hence $w_1 w_2^{-1} \in R_n$, therefore R_n is a subgroup of $E/\{0\}$.

Now since $f(x) = x^n - 1$ has at most n roots, then there are at most n (nth root of unity), therefore R_n is finite, then by some theorem of the direct product of group theory we can conclude that R_n is cyclic group.

(2) Now let E' be the splitting field of $f(x) = x^n - 1$ over E , since p doesn't divide n , then $f'(x) = nx^{n-1} \neq 0$, therefore $f(x)$ is separable and has n distinct roots in E' , let T be the set of all these roots in E' , so by (1) T is also a group. now $R_n \subseteq T \subseteq E'/\{0\}$, but $|T| = n$, hence $|R_n| \mid |T|$, therefore $|R_n|$ divides n .

(3) Now if $f(x)$ splits completely into linear factor in $E[x]$, then $E = E'$ in (2) and that $T = R_n$, then $|R_n| = n$. ■

Example

Back to the example of $f(x) = x^3 - 1 \in \mathbb{Q}[x]$, then $R_3 = \{1\}$ and this is a group of order 1,

let E be the splitting field of $f(x)$ over \mathbb{Q} , then $E = \mathbb{Q}(w)$, then

$R_3 = T = \{1, w, w^2\} = \langle w \rangle = \langle w^2 \rangle$ ◀

Note:

In the previous theorem, we conclude that $R_n = \langle w \rangle$, $|R_n| = n$, then $o(w) = n$, hence w is a primitive n th root of unity, also the converse is true i.e. w is a primitive n th root of unity, then $w \in R_n$ and $w^n = 1$, where n is the smallest such positive integer hence $o(w) = n$ and so $R_n = \langle w \rangle$.

So the generators of R_n are exactly the primitive n th root of unity and there is $\phi(n)$ (euler-phi function) of them.

Theorem

Let F be a field, n is a positive integer, then

(1) there exist a finite field extension $E \mid F$ such that E contains a primitive n th root of unity if and only if $\text{char}(F)$ doesn't divide n .

(2) if $\text{char}(E)$ doesn't divide n , let w be a primitive n th root of unity, then $F(w)$ is the splitting field of $f(x) = x^n - 1 \in F[x]$, and $f(x)$ is separable in $F(w)[x]$ and its roots form a multiplicative cyclic group H such that H is generated by any of primitive n th root of unity in $F(w)$.

Proof:

Let F be a field, n is positive integer.

(1) Assume $p = \text{char}(F)$ doesn't divide n , $f(x) = x^n - 1 \in F[x]$, now $f'(x) = nx^{n-1} \neq 0$, hence $f(x)$ is separable, thus $f(x)$ has n distinct roots in its splitting field E , then $E|F$ is finite field extension, let T be the set of all n th root of unity in E , then $T = \langle w \rangle, o(w) = n, w \in E$, therefore w is a primitive root of unity.

conversely, suppose $E|F$ is finite field extension, let $w \in E$ be a primitive n th root of unity, then $1, w, w^2, \dots, w^{n-1} \in E$ and are all distinct root for $f(x)$, hence $f(x)$ is separable in E thus $f'(x) = nx^{n-1} \neq 0$, therefore $\text{char}(E)$ doesn't divide n .

(2) Assume $p = \text{char}(F)$ doesn't divide n , then by (1) there exist a finite field extension $E|F$ such that E contains a primitive root n th root of unity w , then $1, w, w^2, \dots, w^{n-1} \in E$ are all distinct root for $f(x)$, hence $f(x)$ has n distinct root in $F(w)$, therefore $F(w)$ is the splitting field for $f(x)$ over F , the remaining part of the theorem is clear from the previous theorems. ■

Example

Let $F = \mathbf{Q}$, n is positive integer, $\text{char}(F) = 0$ doesn't divide n , consider $f(x) = x^n - 1 \in \mathbf{Q}[x]$, let $z = re^{i\theta}$ be a root for $f(x)$, then we will have the following roots:

$$1, e^{\frac{2\pi i}{n}}, e^{\frac{3\pi i}{n}}, \dots, e^{\frac{(n-1)\pi i}{n}} \text{ and } E = \mathbf{Q}(e^{\frac{2\pi i}{n}}).$$

Now let us show that $G(E|F)$ is commutative, so let $\sigma, \pi \in G(E|F)$, then

$$\sigma(w), \pi(w) \text{ are also roots for } f(x), \text{ then } \sigma(w) = w^k, \pi(w) = w^l,$$

$1 \leq k, l \leq n-1$, now

$$(\sigma \circ \pi)(w) = \sigma(\pi(w)) = \sigma(w^l) = w^{lk} = (\pi \circ \sigma)(w), \text{ let } y \in E, \text{ then } y \in \mathbf{Q}(w), \text{ then}$$

$$y = a_0 + a_1 w + a_2 w^2 + \dots + a_{n-1} w^{n-1}, a_i \in \mathbf{Q}, \text{ then}$$

$$(\sigma \circ \pi)(y) = \sigma(\pi(y)) = \sigma(\pi(a_0 + a_1 w + a_2 w^2 + \dots + a_{n-1} w^{n-1}))$$

$$= a_0 + a_1 w^{lk} + a_2 w^{2lk} + \dots + a_{n-1} w^{(n-1)lk}$$

$$\text{and so } (\pi \circ \sigma)(y) = a_0 + a_1 w^{lk} + a_2 w^{2lk} + \dots + a_{n-1} w^{(n-1)lk} = (\sigma \circ \pi)(y)$$

hence $G(E|F)$ is commutative Galois group. ◀

Definition

Let F be a field, such that $\text{char}(F)$ doesn't divide n , where n is positive integer.

Let $\{w_1, w_2, \dots, w_m\}$ be the set of all primitive n th roots of unity in the splitting field E for $x^n - 1$ over F , then the polynomial

$\phi_n(x) = (x - w_1)(x - w_2) \dots (x - w_m) \in E[x]$ is called the n th cyclotomic polynomial over F .

Examples

(1) In the previous example where $f(x) = x^3 - 1$, then $w = e^{\frac{2\pi i}{3}}$, since w, w^2 are the only primitive n th root of unity, then it will be the only generators of T , then

$$\phi_3(x) = (x - w)(x - w^2) = x^2 - wx - w^2x + w^3 = x^2 - (w + w^2)x + w^3 = x^2 + x + 1 \in$$

$\mathbb{Z}[x]$ and also we can notice that is irreducible over \mathbb{Q} and $[\mathbb{Q}(w):\mathbb{Q}] = 2 = \deg \phi_2(x)$

(2) the 8th cyclotomic polynomial will be

$\phi_8(x) = (x - w_1)(x - w_2)\dots(x - w_m)$, since the only primitive 8th root of unity are

$$w = w_1 = e^{\frac{2\pi i}{8}}, w_2 = e^{\frac{6\pi i}{8}}, w_3 = e^{\frac{10\pi i}{8}}, w_4 = e^{\frac{14\pi i}{8}}, \text{ hence}$$

$$\phi_8(x) = (x - w_1)(x - w_2)(x - w_3)(x - w_4) = x^4 + 1. \quad \blacktriangleleft$$

Theorem

Let F be a field, n is positive integer and $\text{char}(F)$ doesn't divide n , let $\phi_n(x)$ be the n th cyclotomic polynomial over F , then

$$(1) x^n - 1 = \prod_{d|n, d>0} \phi_d(x)$$

(2) If P is the prime subfield of F , then $\phi_n(x) \in P[x]$

(3) $\deg \phi_n(x) = \varphi(n)$.

Proof:

(1) Let w be a primitive n th root of unity over F , then $F(w)$ is the splitting field of $x^n - 1$ over F , let $d | n$, let $R_d = \{a \in T : o(a) = d\}$, where $o(a)$ is the order of a , now $X = \{R_d : d > 0 \text{ and } d | n\}$ is a partition of T because:

1) since $T \in X$, then $X \neq \emptyset$.

$$2) \bigcup_{\substack{d|n \\ d>0}} R_d = T$$

3) let $a \in R_d \cap R_c$, then $o(a) = d$ and $o(a) = c$, then $c = d$ and $R_d = R_c$.

Now $x^n - 1 = (x - w_1)(x - w_2)\dots(x - w_n)$ in $F(w)[x]$.

$$\begin{aligned} x^n - 1 &= \prod_{w \in T} (x - w) \\ &= \prod_{\substack{d|n \\ d>0}} \prod_{w \in R_d} (x - w) = \prod_{\substack{d|n \\ d>0}} \phi_d(x) \end{aligned}$$

(2) Now $\phi_n(x) = \prod_{w \in R'_n} (x - w)$, $R'_n = \{w \in T : o(w) = n\}$, we will prove the result by the induction on n .

-Basis step: $n=1$, then $\phi_1(x) = (x - 1) \in P[x]$

- Induction step: assume the result hold for all $1 \leq k \leq n$, then for all $d \mid n$, $\phi_d(x) \in P[x]$

$$f(x) = \prod_{\substack{d \mid n \\ 1 \leq d < n}} \phi_d(x) \in P[x]$$

now $x^n - 1 = f(x)\phi_n(x)$ in $F[x]$, by the division algorithm in the Eculidean domain $F[x]$, there exist $q(x), r(x) \in P[x] \subseteq F[x]$ such that:

$$x^n - 1 = q(x)f(x) + r(x) \text{ with } r(x) \equiv 0 \text{ or } \deg r(x) < \deg f(x)$$

$= f(x)\phi_n(x) + 0$ and since this representation is unique, then $r(x) \equiv 0$, there fore $\phi_n(x) = q(x) \in P[x]$.

- (3) $\deg \phi_n(x) =$ number of distinct primitive n th root of unity
 $=$ number of distinct elements of R_n of order n
 $=$ number of generators of R_n
 $= \varphi(n)$. ■

Note: If $f(x) = x^n - 1 \in \mathbb{Q}[x]$, then the n th root of unity are $1, w, w^2, \dots, w^{n-1}$,

where $w = e^{\frac{2\pi i}{n}}$, $\phi_n(x) = \prod_{\substack{1 \leq a < n \\ \gcd(a, n) = 1}} (x - w^a)$

Example

To find $\phi_6(x)$ over \mathbb{Q} , $w = e^{\frac{\pi i}{3}}$

$$\phi_6(x) = \prod_{\substack{1 \leq a < 6 \\ \gcd(a, 6) = 1}} (x - w^a) = (x - e^{\frac{\pi i}{3}})(x - e^{\frac{5\pi i}{3}}) = x^2 - x + 1$$

Note: from now on, we will work in the case when $F = \mathbb{Q}$ and $E = F(w)$, $w = e^{\frac{2\pi i}{n}}$ and let $U_n = \{[a] : \gcd(a, n) = 1\}$ (is a multiplicative group under \times_n)

Theorem

Let $w \in \mathbb{C}$ be a primitive n th root of unity over \mathbb{Q} , let $\phi_n(x)$ be the n th cyclotomic polynomial over \mathbb{Q} , then

- (1) $\phi_n(x) \in \mathbb{Z}[x]$.
- (2) $\phi_n(x)$ is irreducible polynomial over \mathbb{Q} .
- (3) $[\mathbb{Q}(w) : \mathbb{Q}] = \varphi(n)$.
- (4) $G(E | F) \cong U_n$.

Proof:

(1) the proof will be by induction on n .

- Basis step: $n=1$, then $\phi_1(x) = (x-1) \in Z[x]$

- Induction step: assume the result hold for $k, 1 \leq k < n$, then for $1 \leq d < n, d | n$, we have $\phi_d(x) \in Z[x]$.

hence $f(x) = \prod_{\substack{d|n \\ 1 \leq d < n}} \phi_d(x) \in Z[x]$ and so $x^n - 1 = f(x)\phi_n(x) \in Q[x]$

So by the division algorithm (the same way we did in proving the previous theorem) we will get $\phi_n(x) = q(x) \in Z[x]$.

(3) Since $E | F$ is a finite normal and separable field extension, then by the fundamental theorem of Galois,
 $|G(E | F)| = [E:F] = \varphi(n)$, hence $[Q(w):Q] = \varphi(n)$.

(4) since $\phi_n(x) = (x - w_1)(x - w_2) \dots (x - w_{\varphi(n)})$, then for any $\sigma \in G(Q(w) | Q)$, σ permutes the roots of $\phi_n(x)$ i.e. if w is primitive n th root of unity, then $\sigma(w)$ is also primitive n th root of unity and so $\sigma(w) \in \{w^d : 1 \leq d < n, \gcd(n,d)=1\}$, hence for every $\sigma \in G(Q(w) | Q)$, $\sigma_d(w) = w^d, 1 \leq d < n, \gcd(n,d)=1$, now let $\sigma_c, \sigma_d \in G(Q(w) | Q)$ where $1 \leq c, d < n, \gcd(n,c)=1$ and $\gcd(n,d)=1$, now $\sigma_c \circ \sigma_d(w) = \sigma_c(w^d) = w^{cd} = \sigma_{cd}(w)$ and so $\sigma_{cd} = \sigma_c \circ \sigma_d$.

Define the map $\psi : U_n \rightarrow G(Q(w) | Q)$ by

$$\psi([d]) = \sigma_d$$

now let $[c] = [d]$, then $c = d + kn$, some k integer

$$\psi([d]) = \sigma_d$$

$\sigma_d(w) = w^d = w^{c-kn} = w^c = \sigma_c(w)$, hence $\sigma_c = \sigma_d$ therefore ψ is well defined map.

Let $\psi([d]) = \psi([c])$, then $\sigma_c = \sigma_d$

now let $[c], [d] \in U_n$, then by the Euclidean algorithm

$$cd = qn + r, 0 \leq r < n$$

$$[cd] = [r] \text{ and } \sigma_{cd} = \sigma_r, \text{ now}$$

$$\psi([c][d]) = \psi([cd]) = \psi([r]) = \sigma_r = \sigma_{cd} = \sigma_c \sigma_d = \psi([c]) \circ \psi([d])$$

hence ψ is a homomorphism.

now $\ker \psi = \{[d] \in U_n : \psi([d]) = \mathbf{1}\}$

$\psi([d]) = \mathbf{1}$, then $\sigma_d = \mathbf{1}$, therefore $\sigma_d(w) = w^d = w, w^{d-1} = 1$ and

since $o(w) = n$, then $d-1=0$ and therefore $d=1$, then $\ker \psi = \{[1]\}$, hence ψ is one to one homomorphism, since U_n is finite and $G(Q(w) | Q)$ is finite, ψ is onto homomorphism, then ψ is isomorphism map and $G(E | F) \cong U_n$.

(2) Let $\phi_n(x) = f(x)h(x)$, where $f(x)$ is an irreducible factor of $\phi_n(x)$ over Z

(now I have to show $h(x)$ is unit over Z)

Since $\phi_n(x)$ is monic polynomial over Z , so $f(x)$ and $h(x)$.

Let w be a root for $f(x)$, then w is a root for $\phi_n(x)$, hence w is a primitive n th root of unity.

Let p be a prime such that p doesn't divide n i.e. $\gcd(p,n)=1$, hence w^p is also a primitive n th root of unity and also generator for R_n .

we claim that w^p is a root for $f(x)$.

suppose this is not the case i.e. w^p is not a root for $f(x)$, then $\phi_n(w^p) = 0$

implies $f(w^p)h(w^p) = 0$, hence w^p is a root for $h(x)$, therefore w is a root for $h(x^p)$, because $f(x)$ is irreducible polynomial over \mathbf{Q} and $f(w)=0$ and $h(w^p)=0$, hence $f(x) \mid h(x^p)$, therefore $h(x^p)=f(x)g(x)$ some $g(x) \in \mathbf{Q}[x]$.

by division algorithm over $\mathbf{Z}[x]$, there exist $q(x), r(x) \in \mathbf{Z}[x]$,

$h(x^p)=f(x)q(x)+r(x)$, $r(x) \equiv 0$ or $\deg r(x) < \deg f(x)$, by the uniqueness of this expression we have $r(x) \equiv 0$ and therefore $g(x)=q(x) \in \mathbf{Z}[x]$.

Now for any $t(x) \in \mathbf{Z}[x]$, let $\overline{t(x)} \in \mathbf{Z}_p[x]$ be the corresponding polynomial by taking modulo n to the coefficients of $t(x)$.

Now $\overline{h(x^p)} = \overline{a_0 + a_1x^p + \dots + a_sx^{ps}}$, since $\text{char}(\mathbf{Z}_p)=p$, then

$\overline{h(x^p)} = (\overline{a_0 + a_1x + \dots + a_sx^s})^p = \overline{(h(x))^p}$, hence $\overline{(h(x))^p} = \overline{h(x^p)} = \overline{f(x)g(x)}$, hence \overline{w}

is common root for both $\overline{h(x)}$ and $\overline{h(x^p)}$, now

$\overline{\phi_n(x)} = \overline{f(x)g(x)}$ and $\phi_n(x) \mid x^n - 1$, then $\overline{(x^n - 1)} = x^n - [1] \in \mathbf{Z}_p[x]$

have a multiple root (one from $\overline{f(x)}$ and one from $\overline{h(x)}$) say a is a root of

$t(x) = x^n - [1]$, then $t'(x) = [n]x^{n-1} = [0]$ so either $[n] = [0]$ (impossible since

$\gcd(p,n)=1$) or $a^{n-1} = [0]$, hence $a^{n-1} \equiv 1 \pmod{p}$ which is by fermat's theorem

implies $a \equiv 0 \pmod{p}$, so $a = [0]$ but $t(a) = [0]^n - [1] \neq [0]$, A contradiction, hence

w^p is a root for $f(x)$ and by the induction we can show w^{p^r} is also a root of $f(x)$

for any r positive integer and also $w^{p_1^{r_1}p_2^{r_2}\dots p_s^{r_s}}$ is also a root for $f(x)$ for distinct primes p_i 's don't divide n .

So now any primitive root of unity w^d , $1 \leq d < n$, $\gcd(d,n)=1$ is a root for $f(x)$

since d can be factored into its canonical form as product of primes hence it is clear that

$\phi_n(x) = f(x)$ and so $\phi_n(x)$ is irreducible over \mathbf{Z} and hence it is irreducible over \mathbf{Q} . ■

Corollary:

Let n be positive integer, then for every $m \mid n$ $\frac{x^n - 1}{x^m - 1} \in \mathbf{Z}[x]$, moreover if

$1 < m < n$, then $\phi_n(x) \mid \frac{x^n - 1}{x^m - 1}$.

Proof:

since $x^n - 1 = \prod_{\substack{d|n \\ d>0}} \phi_d(x)$, since $m | n$, then

$$x^n - 1 = \prod_{\substack{d|n \\ d>0 \\ d \neq m}} \phi_d(x) \phi_m(x) = (x^m - 1) \prod_{\substack{d|n \\ d>0 \\ d \neq m}} \phi_d(x) \prod_{\substack{s|m \\ s>0}} \phi_s(x), \text{ then}$$

$$\frac{x^n - 1}{x^m - 1} = \prod_{\substack{d|n \\ d>0 \\ d \neq m}} \phi_d(x) \prod_{\substack{s|m \\ s>0}} \phi_s(x) \in \mathbf{Z}[x].$$

Now assume $1 < m < n$, then $\frac{x^n - 1}{x^m - 1} = \phi_n(x) \prod_{\substack{d|n \\ d>0 \\ d \neq m \\ d \neq n}} \phi_d(x) \prod_{\substack{s|m \\ s>0}} \phi_s(x)$

Hence $\phi_n(x)$ divides $\frac{x^n - 1}{x^m - 1}$. ■

Examples

(1) Since $4 | 20$, then $\frac{x^{20} - 1}{x^4 - 1} \in \mathbf{Z}[x]$.

(2)

a) find the Galois group of $f(x) = x^2 - x + 1$ over \mathbf{Q} .

As we did before, $f(x) = \phi_6(x) = x^2 - x + 1$, now $w = e^{\frac{2\pi i}{6}} = e^{\frac{i\pi}{3}}$, then the primitive

6th root of unity are $\{w^d : 1 \leq d < n, \gcd(d, 6) = 1\} = \{w, w^5\} = \{e^{\frac{i\pi}{3}}, e^{\frac{5i\pi}{3}}\}$, the splitting field E of $\phi_6(x)$ over \mathbf{Q} is $E = \mathbf{Q}(w, w^5) = \mathbf{Q}(w)$, but $G(E | \mathbf{Q}) \cong U_6$ so $|G(E | \mathbf{Q})| = 2$, so if $\sigma \in G(E | \mathbf{Q})$, then σ either the identity automorphism or $\sigma(w) = w^5$, so $G(E | \mathbf{Q}) = \{\mathbf{1}, \sigma_5\}$ where $\sigma_5(q_0 + q_1 w) = q_0 + q_1 w^5$.

b) Show that the Galois group of $x^4 - 1$ and $x^2 - x + 1$ are isomorphic.

Since the splitting field of $x^4 - 1$ over \mathbf{Q} is $E' = \mathbf{Q}(w')$, $w' = e^{\frac{i\pi}{2}}$

$[E' : \mathbf{Q}] = \deg(w', \mathbf{Q}) = 2$, since $E' | \mathbf{Q}$ is finite separable and normal extension, therefore $|G(E' | \mathbf{Q})| = 2$, hence $|G(E' | \mathbf{Q})| \cong U_2$ and therefore $G(E | \mathbf{Q}) \cong G(E' | \mathbf{Q})$.

(3) Let p a prime integer, then

$$x^p - 1 = \prod_{\substack{d|p \\ d>0}} \phi_d(x), \text{ then } (x^p - 1) = (x - 1) \phi_p(x)$$

So $\phi_p(x) = 1 + x + x^2 + \dots + x^{p-1} \in \mathbf{Z}[x]$ ◀

§ 3.2 The Galois Group of a Cubic Polynomial

Definition

Given $f(x) \in F[x]$, the Galois group of $f(x)$ is the Galois group of its splitting field over F .

We will start this section by **(1)** showing Galois group of the polynomial $f(x) = x^3 - 5$ over \mathbf{Q} is isomorphic to S_3 and **(2)** Finding the Galois group of $\mathbf{Q}(\sqrt[3]{5}, \frac{-1+i\sqrt{3}}{2}) | \mathbf{Q}$ and Finding T and $S(G)$ as described in the fundamental theorem of Galois theory.

Example

(1) Since $f(x) = x^3 - 5$ is irreducible over \mathbf{Q} because of the irreducibility over \mathbf{Z} (by Eisenstein's criterion with $p=5$).

Let E be the splitting field for $f(x)$ over \mathbf{Q} , then $f(x)$ over E will be

$$f(x) = x^3 - 5 = (x - \sqrt[3]{5})(x - \sqrt[3]{5} \frac{-1+i\sqrt{3}}{2})(x - \sqrt[3]{5} \frac{-1-i\sqrt{3}}{2}),$$

now let $c = \sqrt[3]{5}$, $w = \frac{-1+i\sqrt{3}}{2}$, then $E = \mathbf{Q}(c, cw, c\bar{w}) = E(c, w)$.

Since the Galois group of $f(x)$ is the Galois group of $E | \mathbf{Q}$, hence $E | \mathbf{Q}$ is a finite normal and separable extension.

Now $\text{irr}(w, \mathbf{Q}(c)) = x^2 + x + 1$ (because $w^2 + w + 1 = 0$), $\text{deg}(w, \mathbf{Q}(c)) = 2$.

$$\text{irr}(c, \mathbf{Q}) = x^3 - 5, \text{deg}(c, \mathbf{Q}) = 3.$$

$$[\mathbf{Q}(c, w) : \mathbf{Q}] = [\mathbf{Q}(c, w) : \mathbf{Q}(c)][\mathbf{Q}(c) : \mathbf{Q}] = 2 \cdot 3 = 6 = 3!.$$

$$\text{hence } |G(E | \mathbf{Q})| = [E : \mathbf{Q}] = 6.$$

Now $G = G(E | \mathbf{Q})$ is a group of automorphisms of order 6, so either $G \cong (Z_6, +_6)$ or $G \cong (S_3, \circ)$.

Now if $G \cong (Z_6, +_6)$:

Since $[\mathbf{Q}(c) : \mathbf{Q}] = [\mathbf{Q}(cw) : \mathbf{Q}] = 3$, then by the fundamental theorem of Galois we have

$$[\mathbf{Q}(c) : \mathbf{Q}] = [G(E | \mathbf{Q}) : G(E | \mathbf{Q}(c))] = \frac{|G(E | \mathbf{Q})|}{|G(E | \mathbf{Q}(c))|}, \text{ then } 3 = \frac{6}{|G(E | \mathbf{Q}(c))|}$$

$$\text{therefore, } |G(E | \mathbf{Q}(c))| = 2$$

$$\text{and by the same way } |G(E | \mathbf{Q}(cw))| = |G(E | \mathbf{Q}(cw^2))| = 2$$

but Z_6 has only one subgroup $\{[0], [3]\}$ of order 2

So G is not isomorphic to $(Z_6, +_6)$, and therefore $G \cong (S_3, \circ)$.

(2) To find the Galois group of $E = \mathbf{Q}(c, w)$, let $\sigma \in G(E | \mathbf{Q})$, then $\sigma(c)$ will have three possibilities c, cw, cw^2 and $\sigma(w)$ will have only two possibilities w, w^2 , so we have :

$\sigma_1(c) = c$ $\sigma_1(w) = w$	$\sigma_2(c) = cw$ $\sigma_2(w) = w$
$\sigma_3(c) = cw^2$ $\sigma_3(w) = w$	$\sigma_4(c) = c$ $\sigma_4(w) = w^2$
$\sigma_5(c) = cw$ $\sigma_5(w) = w^2$	$\sigma_6(c) = cw^2$ $\sigma_6(w) = w^2$

and these are the elements of $G(E | \mathbf{Q})$.

To find $\psi(\mathbf{Q}(w)) = G(E | \mathbf{Q}(w))$, let for instance $L = \mathbf{Q}(w), F = \mathbf{Q}$, then

$$|G(L | F)| = \frac{|G(E | F)|}{[E : L]} = \frac{6}{2} = 3, \text{ thus } G(L | F) \text{ has three automorphisms,}$$

let $a \in \mathbf{Q}(w), \sigma \in G(L | F)$ such that $\sigma(a) = a$, then

$\sigma(c + dw) = c + dw$, then $c + d\sigma(w) = c + dw$, therefore σ is either

$\mathbf{1} = \sigma_1, \sigma_2$ or σ_3 . Hence $G(L | F) = \{\mathbf{1}, \sigma_2, \sigma_3\} = \psi(\mathbf{Q}(w))$

and by the same way for the other subfields of E we will reach the following diagram :

Subgroup of $G(E F)$	Fixed field
$\{\mathbf{1}\}$	$E = \mathbf{Q}(c, w)$
$\{\mathbf{1}, \sigma_5\}$	$\mathbf{Q}(cw)$
$\{\mathbf{1}, \sigma_4\}$	$\mathbf{Q}(c)$
$\{\mathbf{1}, \sigma_6\}$	$\mathbf{Q}(cw^2)$
$\{\mathbf{1}, \sigma_2, \sigma_3\}$	$\mathbf{Q}(w)$
$\{\mathbf{1}, \sigma_2, \sigma_3, \dots, \sigma_6\}$	\mathbf{Q}

In this example we can take advantage of having $G(E | F) \cong (S_3, \circ)$

by noting that S_3 has 3 nontrivial subgroups:

$H_1 = \{(\mathbf{1}), (1\ 2)\}, H_2 = \{(\mathbf{1}), (1\ 3)\}, H_3 = \{(\mathbf{1}), (2\ 3)\}$ and $H_4 = \{(\mathbf{1}), (1\ 2\ 3), (1\ 3\ 2)\}$

and note that $[S_3 : H_4] = 2$, then the corresponding subfield L of H_4 must be $[E : L] = 2 = [S_3 : H_4] = [G(E | F) : G(E | L)]$, hence $L = \mathbf{Q}(w)$.

Also $[\mathbf{Q}(cw) : \mathbf{Q}] = [\mathbf{Q}(cw^2) : \mathbf{Q}] = 3$ and

$$[S_3 : H_1] = [S_3 : H_2] = [S_3 : H_3] = 3.$$

let $a_1 = c, a_2 = cw$ and $a_3 = cw^2$, then

$$(1\ 2) : a_1 \rightarrow a_2$$

$$a_2 \rightarrow a_1 \Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ a_1 & a_2 & a_3 \end{pmatrix}, \text{ hence}$$

$$a_3 \rightarrow a_3$$

H_1 corresponds to $\mathbf{Q}(cw^2)$, because $a_3 = cw^2$ is left fixed

H_2 corresponds to $\mathbf{Q}(cw)$, because $a_2 = cw$ is left fixed

H_3 corresponds to $\mathbf{Q}(c)$, because $a_1 = c$ is left fixed. ◀

Now the immediate question that arise from this example is it always the Galois group of any separable irreducible cubic polynomial isomorphic with S_3 or not?

The answer is no as we will see in the subsequent work.

So let F be a field with $\text{char}(F) \neq 3$, consider the cubic polynomial $f(x) = x^3 + ax^2 + bx + c \in F[x]$,

Let $x = u - \frac{a}{3}$, then

$$\begin{aligned} g(u) = f\left(u - \frac{a}{3}\right) &= \left(u - \frac{a}{3}\right)^3 + a\left(u - \frac{a}{3}\right)^2 + b\left(u - \frac{a}{3}\right) + c \\ &= u^3 - au^2 + \frac{a^3}{3}u - \frac{a^3}{27} + au^2 - \frac{2a^2}{3}u + \frac{a^3}{9} + bu - \frac{ab}{3} + c \\ &= u^3 + (-9 + a)u^2 + \left(\frac{a^2}{3} - \frac{2a^2}{3} + b\right)u + \left(-\frac{a^3}{27} + \frac{a^3}{9} - \frac{ab}{3} + c\right) \\ &= u^3 + \left(b - \frac{a^2}{3}\right)u + \left(c + \frac{2a^3}{27} - \frac{ab}{3}\right) \end{aligned}$$

Hence if r is a root for $g(u)$, then $r - \frac{a}{3}$ is a root of $f(x)$.

So for any cubic polynomial, we can eliminate the quadratic term to have a polynomial $f(x) = x^3 + bx + c \in F[x]$, then $f(x)$ is irreducible if and only if $f(x)$ has no zero in F .

Let E be the splitting field for $f(x)$ over F , then

$$f(x) = (x - a_1)(x - a_2)(x - a_3) \text{ in } E[x].$$

$$f(x) = (x^2 - (a_1 + a_2)x + a_1a_2)(x - a_3)$$

$$= x^3 - (a_1 + a_2)x^2 + a_1a_2x - a_3x^2 + (a_1a_3 + a_2a_3)x - a_1a_2a_3 = x^3 + bx + c$$

and by comparing the coefficients of $f(x)$, we will have

$$a_1 + a_2 + a_3 = 0, \quad a_1a_2 + a_1a_3 + a_2a_3 = b, \quad -a_1a_2a_3 = c$$

Definition

Given $f(x) \in F[x]$ a cubic separable polynomial with a_1, a_2 and a_3 as its roots in its splitting field E , the discriminant D of $f(x)$ by

$$D = [(a_1 - a_2)(a_1 - a_3)(a_2 - a_3)]^2 = d^2, \quad d = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3).$$

Now let $\sigma \in G(E|F)$, then σ fixes F , consider

$$\sigma(d) = \sigma((a_1 - a_2)(a_1 - a_3)(a_2 - a_3)) = (\sigma(a_1) - \sigma(a_2))(\sigma(a_1) - \sigma(a_3))(\sigma(a_2) - \sigma(a_3))$$

since σ is just a permutation on the roots of $f(x)$, then

$$\text{either } \sigma(d) = d \text{ or } \sigma(d) = -d, \text{ hence } \sigma(D) = \sigma(d^2) = [\sigma(d)]^2 = D.$$

hence σ leaves D fixed, now to find D in terms of b and c we will have to work a lot in just simplification and the result will be

$$D = -4b^3 - 27c^2.$$

Theorem

Let $f(x) = x^3 + bx + c$ be an irreducible and separable polynomial in $F[x]$, let E be the splitting field for $f(x)$ over F and $G = G(E|F)$ be the Galois group of $f(x)$, then

$G \cong S_3$ if and only if D is not a square in F .

Moreover if D is a square in F , then $[E:F] = 3$ and $G \cong A_3$.

Proof:

(our goal in the proof to show $G \cong A_3$ if and only if $d \in F$.)

Let $f(x) = x^3 + bx + c$ be an irreducible and separable polynomial over F , since $D = -4b^3 - 27c^2$, then $D \in F$.

let $\sigma \in G$, then assume D is a square in F i.e. $d \in F$, then $\sigma(d) = d$, thus σ can't be an odd permutation (because there are only 3 roots and $\sigma(d) = d$ means either no change for them or only 2 have been changed)

then $\sigma \in A_3$, $G \subseteq A_3$.

Now let $\sigma \in A_3$, then $\sigma(d) = d$, since $f(x)$ is separable and irreducible the three roots of $f(x)$ are distinct and therefore $G \neq \{1\}$ thus $G = A_3$.

By the same way if $G = A_3$, then $d \in F$,

hence $G \cong S_3$ if and only if $d \notin F$.

Now if $d \in F$, then $G = A_3$, $|G| = 3$, by the fundamental theorem of Galois, $[E:F] = |G| = 3$. ■

Theorem

Let $f(x) = x^3 + bx + c$ be an irreducible and separable polynomial over the field F , let E be the splitting field for $f(x)$ over F , then $E = F(\sqrt{D}, r)$ for any root r to $f(x)$.

Proof:

Let r be a root for $f(x)$ over F , then $\deg(r, F) = 3$ and hence $[F(r) : F] = 3$, if $E = F(r)$, then $E = F(\sqrt{D}, r)$

suppose $F(r) \subset E$, then $[E : F] = 6$ because $[E : F] = [E : F(r)][F(r) : F]$, where $\text{irr}(d, F(r)) = x^2 - 1$ and therefore $\deg(d, F(r)) = 2$

so $[E : F] = 2(3) = 6$, hence $G(E | F) \cong S_3$, then $d \notin F$ so $E = F(\sqrt{D}, r)$. ■

Example

Consider $x^3 - 3x + 2 \in \mathbb{Q}[x]$, then $x^3 - 3x + 2$ is an irreducible over \mathbb{Q} by Eisenstein's criterion, now $D = -4b^3 - 27c^2 = 148$, thus D is not square in \mathbb{Q} , hence

$G(E | \mathbb{Q}) \cong S_3$ and $E = \mathbb{Q}(\sqrt{148}, r)$, r is a root for $f(x)$. ◀

REFERENCES

1-D.S.Malik, John N.Mordeson and M.K.Sen.

Fundamentals of Abstract algebra. McGraw-Hill, 1997.

2-David S.Dummit and Richard Foote.

Abstract Algebra, 2nd Ed. Upper Saddle River, New Jersey: Prentice Hall, 1999.

3-John B.Fraleigh.

A First Course in Abstract Algebra. Addison Wesley, 2003.

4-I.N.Herstein.

Topics in Algebra, 2nd Ed. John Wiley & sons, 1975.

5-Surjeet Singh and Qazi Zameeruddin.

Modern Algebra, 6th Ed. Vikas Publishing House, 1988.