



Ministry of Higher Education and Scientific Research

Al- Qadisiya University

College of Computer Science and Mathematics

Department of Mathematics

Galois theory

A research submitted to

Al Qadisiya University- College of Computer Science and
Mathematics- Department of Mathematics in partial
fulfillment of the requirements for the degree of B.S.C. in
Science mathematical.

By

Ayat ali safar

supervised

Sahar Jaafar with her master degree

٢٠١٧م

١٤٣٤ هـ

بسم الله الرحمن الرحيم

((ويسألونك عن الروح قبل الروح من أمر ربي وما أوتيت من العلم إلا

قليلا))

صدق الله العلي العظيم

(الأسراء 85)

بسم الله الرحمن الرحيم

((يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات))

صدق الله العلي العظيم

(المجادله 11)

الإهداء

أهدي ثمرة جهدي هذا
إلى مهد الحضارة ومهبط الأنبياء ... إلى أرض الشهداء والتضحيات
العراق .. العظيم

إلى من جرع الكأس فارغاً ليسقيني قطرة حب
إلى من كلت أنامله ليقدّم لنا لحضه سعادة
إلى من حصد الأشواق عن دربي ليمهد لي طريق العلم
إلى القلب الكبير والدي العزيز

إلى من أرضعني الحب والحنان
إلى رمز الحب وبلسم الشفاء
إلى القلب الناصع بالبياض
والدتي .. الحبيبة

إلى الذين بذلوا كل جهد وعطاء لكي أصل إلى هذه اللحظة
أساتذتي .. الكرام
الأساتذة الفاضلة سحر جعفر

شكر وتقدير

كل الشكر والثناء لله سبحانه تعالى لأن التوفيق من عند الله في مثل هذه
اللحظات يتوقف القلم

ليفكر قبل أن يخط الحروف ليجمعها في كلمات تبعث الحرف وعبثاً أن يحاول
تجميعها في سطور

سطوراً كثيرة تمر في الخيال ولا يبقى لما في نهاية المطاف الا قليل من الذكريات
وصور تجمعا برفاق كانوا جانبنا

فواجبا علينا شكرهم ووداعهم ونحن نخطو خطوتنا الاولى في غمار الحياة
ونحنس يجرى الشكر والعرفان الي كل من اشعل شمع في دروب عملنا
والي من وقف علي المنابر واعطى من حصيلة فكره لينير دربنا
الي الاساتذة الكرام في كلية علوم الحاسوب وتكنولوجيا المعلومات
توجه بالشكر الجزيل الي

الاستاذة الفاضلة . . . سحر جعفر

الذي تفضل بالإشراف علي هذا البحث فجزاه الله عنا كل خير فله منا كل التقدير
والاحترام

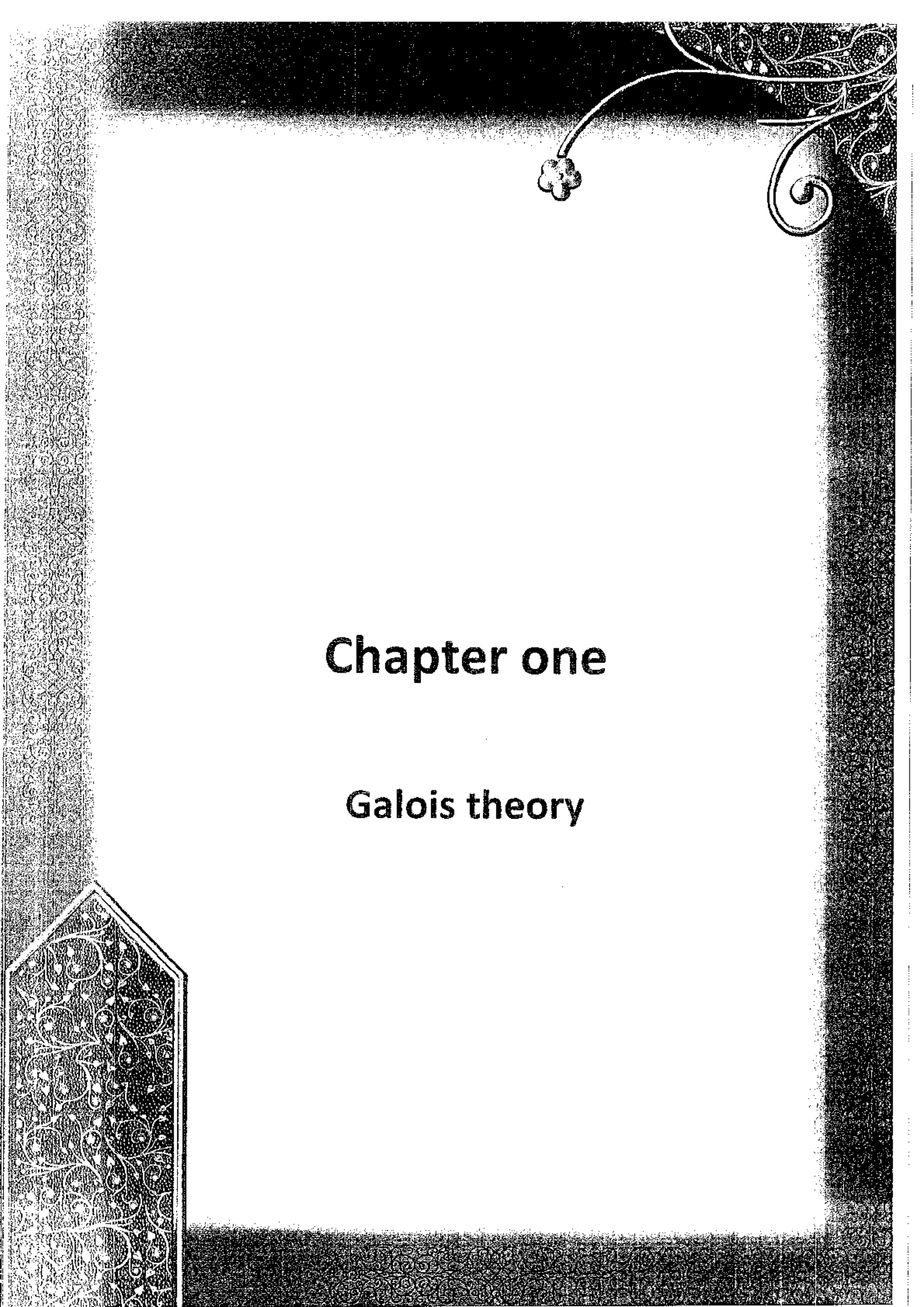
Contents	Pages
Chapter one	1
1-1 theorem	2
1-2 lemma dedekind	3
1-3 theorem	8
1-4 fundametal theorem of galois theory	12
1-5 fundamental theorem of algebra	19
Chapter two	21
2-1 application of galois theory	21
2-2 deffinition	24
2-3 cyclic extensions	27

... Abstract ...

Galois used Permutation groups to describe how the various roots of a given Polynomial equation are related to each other. The modern approach to Galois theory developed by Richard Dedekind, Leopold Kronecker among others, involves studying automorphisms of field extensions. Further abstraction of Galois theory is achieved by the theory of Galois connections. Application to classical problems.

⌘ Introductions ⌘

In this chapter we deal with the central results of Galois theory. The Fundamental theorem on Galois theory establishes a one-to-one correspondence between the set of subfields of E , where E is a splitting field of a separable polynomial in $F[x]$ and the set of subgroups of the group of F -automorphisms of E . This correspondence transforms certain problems about subfields of fields into more amenable problems about subgroups of groups. Among the applications, this serves as the basis of Galois' criterion for solvability of an equation by radicals.



Chapter one

Galois theory

- chapter one -

1 Automorphism groups and Fixed fields

Let E be an extension of a field. We denote by $G(E/F)$ the group of automorphisms of E leaving each element of F fixed. The group $G(E/F)$ is also called the group of F -automorphisms of E . Throughout this section we confine ourselves to finite separable extensions and their groups of automorphisms. We recall that a finite separable extension E of F is simple. Thus, $E = F(\alpha)$ for some $\alpha \in E$. Let $P(x)$ be the minimal polynomial of α over F . Then $[F(\alpha):F] = \text{degree of } P(x) = n$, say. Also we get that the order of the group $G(E/F)$ is $\leq n$. Thus we have.

Theorem (1.1) If E is a finite extension of a field F , then $|G(E/F)| \leq [E:F]$.

Example

A - Consider $G = G(C/R)$ if $a+ib \in C$

$$\begin{aligned} & a+ib \in R \text{ and } \sigma \in G \text{ then } \sigma(a+ib) = \sigma(a) + \sigma(i)\sigma(b) \\ & = a + \sigma(i)b \quad \text{Also } (-1) = \sigma(-1) = \sigma(i^2) = (\sigma(i))^2 \end{aligned}$$

thus $\sigma(i) = \pm i$. Hence $\sigma(a+ib) = a \pm ib$. Thus

There are only two possible R -automorphisms of C Hence $|G| = 2$ In this case $[C:R] = 2$ also

B

consider $G = G(Q(\sqrt[3]{2})/Q)$. $x^3 - 2$ is the

minimal Polynomial for $\sqrt[3]{2}$ over Q So

$[Q(\sqrt[3]{2}) : Q] = 3$ and $Q(\sqrt[3]{2})$ has basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

Over Q , let $\sigma : Q(\sqrt[3]{2}) \rightarrow Q(\sqrt[3]{2})$ be an

auto morphism such that $\sigma(a) = a$ for all $a \in Q$

Then

$$\begin{aligned}\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= \sigma(a) + \sigma(b)\sigma(\sqrt[3]{2}) + \sigma(c)\sigma(\sqrt[3]{4}) \\ &= a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{4})\end{aligned}$$

Also $(\sigma(\sqrt[3]{2}))^3 = \sigma((\sqrt[3]{2})^3) = \sigma(2) = 2$

So $\sigma(\sqrt[3]{2})$ is a cube root of 2. Therefore,

$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \sqrt[3]{2}\omega \text{ or } \sqrt[3]{2}\omega^2, \text{ where } \omega = \sqrt[3]{-1}, \omega^3 = 1, \omega \neq 1$$

$\omega \neq 1$ because $\sigma(\sqrt[3]{2})$ is real, the only possibility

is $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Hence σ is the identity. Thus,

$G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group.

Definition

Let H be any field, and let H be a subgroup of the

group of automorphisms of E . Then the set $E_H =$

$\{x \in E \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ is called the fixed

field of the group of automorphisms H .

It's easy to verify that E_H is a subfield of E

if E is an extension of a field F and $H \leq G(E/F)$

Then $(F \subseteq E_H \subseteq E)$ for example.

$(H = \mathbb{R}$ where $H = G(\mathbb{C}/\mathbb{R})$, and $\mathbb{Q}(\sqrt[3]{2})_H = \mathbb{Q}(\sqrt[3]{2})$ where $H = G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ one of the main results this section is

Lemma (Dedekind 1-2)

~~~~~  
Let  $F$  and  $E$  be fields, and let  $\sigma_1, \sigma_2, \dots, \sigma_n$  be distinct embeddings of  $F$  into  $E$ . Suppose that, for  $a_1, a_2, \dots, a_n \in E$  ( $\sum_{i=1}^n a_i \sigma_i(a) = 0$ ) for all  $a \in F$ . Then  $\{a_i = 0\}$  for all  $i = 1, 2, \dots, n$  (This also expressed by saying that distinct embeddings of  $F$  into  $E$  are linearly independent over  $E$ ).

Proof

Suppose there exist elements  $a_1, \dots, a_n \in E$  not all zero such that  $a_1 \sigma_1(x) + \dots + a_n \sigma_n(x) = 0$  for all  $x \in F$ . of all the equations of the form (1) there must be at least one for which the number of non zero terms is least. let

$b_1 \sigma_1(x) + \dots + b_m \sigma_m(x) = 0$  for all  $x \in F$ , be such a relation, where  $b_i \in E$ ,  $i = 1, \dots, m$ , and no  $b_i = 0$  clearly,  $m \geq 1$ .

Because  $\sigma_1 \neq \sigma_m$  there exist  $y \in F$  such that  $\sigma_1(y) \neq \sigma_m(y)$ . Replace  $x$  by  $yx$  in (2) and obtain  $b_1 \sigma_1(yx) + \dots + b_m \sigma_m(yx) = 0$

for all  $x \in F$  but this implies.

$$b_1 \sigma_1(y) - \sigma_1(x) + m + b_m \sigma_m(y) - \sigma_m(x) = 0 \rightarrow (3)$$

For all  $x \in F$  if we multiply (2) by  $\sigma_1(y)$  and subtract from (3), we get

$$b_2(\sigma_1(y) - \sigma_2(y)) - \sigma_2(x) + m + b_m(\sigma_1(y) - \sigma_m(y)) - \sigma_m(x) =$$

The coefficient of  $\sigma_m(x)$  is  $b_m(\sigma_1(y) - \sigma_m(y)) \neq 0$

So we have an equation of (1) with fewer than  $m$  terms, a contradiction in view of the choice of relation (2) in this proof.

**Theorem:** Let  $H$  be a finite subgroup of the automorphisms of a field  $E$ . Then  $[E : E^H] = |H|$ .

Proof:

Let  $H = \{e = g_1, \dots, g_n\}$  and let  $[E : E^H] = m$  if possible, suppose  $m < n$ . Let  $\{a_1, \dots, a_m\}$  be a basis for  $E$  over  $E^H$ . Consider the system of  $m$  homogeneous linear equations,

$$g_1(a_j)x_1 + \dots + g_n(a_j)x_n = 0 \quad j = 1, 2, \dots, m$$

in  $n$  unknowns  $x_1, \dots, x_n$  because  $n > m$  this system has a nontrivial solution. So there exist  $y_1, \dots, y_n \in E$ , not all zero, such that

$$g_1(a_j)y_1 + \dots + g_n(a_j)y_n = 0 \quad \rightarrow (1)$$

$j = 1, \dots, m$ . Let  $\alpha$  be any element of  $E$ . Then

$$\alpha = \alpha_1 a_1 + \dots + \alpha_m a_m$$

where  $\alpha_1, \dots, \alpha_m \in E^H$ . So

$$\begin{aligned}
 g_1(a)y_1 + \dots + g_n(a)y_n &= g_1\left(\sum_{i=1}^m \alpha_i a_i\right)y_1 + \dots + g_n\left(\sum_{i=1}^m \alpha_i a_i\right)y_n \\
 &= \sum_{i=1}^m \alpha_i g_1(a_i)y_1 + \dots + \sum_{i=1}^m \alpha_i g_n(a_i)y_n \\
 &= \sum_{i=1}^m \alpha_i (g_1(a_i)y_1 + \dots + g_n(a_i)y_n) = C
 \end{aligned}$$

- suppose if possible  $m > n$ . Then there exist a set of  $n+1$  elements of  $E$  that are linearly independent over  $E_H$ ; let such a set be  $a_1, \dots, a_{n+1}$ . Consider the family of  $n$  homogeneous linear equations.

$g_j(a_1)x_1 + \dots + g_j(a_{n+1})x_{n+1} = 0, \quad j = 1, \dots, n$   
in  $n+1$  unknowns  $x_1, \dots, x_{n+1}$ , so there exist  $y_1, \dots, y_{n+1} \in E$ , not all zero such that

$g_j(a_1)y_1 + \dots + g_j(a_{n+1})y_{n+1} = 0 \implies (2)$   
 $j = 1, \dots, n$  choose  $y_1, \dots, y_{n+1}$  so that as few as possible are non zero, and renumber so that  $y_i \neq 0, i = 1, \dots, r$  and  $y_{n+1} = 0 = \dots = y_{n+1}$ .  
Equations (2) now becomes

$$g_j(a_1)y_1 + \dots + g_j(a_r)y_r = 0 \implies (3)$$

let  $g \in E_H$  and operate on (3) with  $g$ . This gives a system of equations

$$g g_j(a_1)g(y_1) + \dots + g g_j(a_r)g(y_r) = 0 \implies (4)$$

if we multiply relations (3) by  $g(y_1)$ , and (4) by  $y_1$ , and subtract, we obtain

$$g_j(a_2)(y_2 g(y_1) - g(y_2) y_1) + \dots + g_j(a_r)(y_r g(y_1) - g(y_r) y_1) = 0 \implies (5)$$

#  $j=1, \dots, r$  (5) is a system of equations like (3) but with fewer terms. which gives a contradiction unless all the coefficients  $y_i g(y_i) - y_i g(y_i)$  are equal to zero. if this happens, then  $y_i y_i^{-1} = g(y_i y_i^{-1})$  for all  $g \in H$ . Thus  $y_i y_i^{-1} \in E_H$ . Therefore there exist  $z_1, \dots, z_r \in E_H$  such that  $y_i = y_i z_i$ ,  $i=1, \dots, r$ . Then relation (3) with  $j=1$  becomes  $g_1(a_1) y_1 z_1 + \dots + g_1(a_r) y_1 z_r = 0$

This implies

$$g_1(a_1) z_1 + \dots + g_1(a_r) z_r = 0$$

because  $y_1 \neq 0$ . But then because  $z_i \in E_H$ ,  $i=1, \dots, r$  we get  $g_1(a_1 z_1) + \dots + g_1(a_r z_r) = 0$

So

$$a_1 z_1 + \dots + a_r z_r = 0$$

because  $g_1$  is a non-zero embedding. But the linear independence  $a_1, \dots, a_r$  over  $E_H$  yields that  $z_1 = \dots = z_r = 0$ . This implies  $y_1 = \dots = y_r = 0$  a contradiction.

Thorem 3

— let  $E$  be a finite separable extension of a field  $F$ , and  $H < G(E/F)$  Then  $G(E/E_H) = H$  and  $[E : E_H] = |G(E/E_H)|$

Proof

Clearly  $H < G(E/E_H)$ , By  
 $|H| = [E:E_H]$  Also by Theorem (1.1) we have

$$|H| = [E:E_H] \geq |G(E/E_H)| \geq |H|$$

Hence  $H = G(E/E_H)$  and  $[E:E_H] = |G(E/E_H)|$

This completes the proof

Theorem 1-3, let  $E$  be a finite separable extension of  
a field  $F$ . The following are equivalent

- (i)  $E$  is a normal extension of  $F$
- (ii)  $F$  is the fixed field of  $G(E/F)$
- (iii)  $[E:F] = |G(E/F)|$

Proof

because  $E$  is a finite separable extension of  
 $F \Rightarrow E = F(\alpha)$  for some  $\alpha \in E$ . Let  $P(x)$  be the minimal  
polynomial of  $\alpha$  over  $F$  and let its degree be  $n$ . Then

$$[E:F] = [F(\alpha):F] = n \quad (1)$$

Also if  $E_0$  is the fixed field of  $G(E/F)$  then by

Theorem 11.4

$$[E:E_0] = |G(E/F)|$$

because  $E$  is a separable extension of  $F$   $\alpha \in E$  is a separable element, so its minimal polynomial  $P(x)$  over  $F$  must have distinct roots. So the number of distinct roots of  $P(x)$  is equal to  $n$ . In addition because  $E = F(\alpha)$  is a normal extension of  $F$ , any embedding  $\sigma: F(\alpha) \rightarrow \bar{F}$  shall map  $F(\alpha)$  onto  $F(\alpha)$ . clearly, any member of  $G(E/F)$  is an extension of the inclusion mapping  $F \rightarrow \bar{F}$

$|G(E/F)| = \text{number of distinct roots of } P(x) = n$

Thus (1)-(3) give

$$[E:F] = n = |G(E/F)| = [E:E_0]$$

Hence  $[E_0:F] = 1 \Rightarrow$  So  $E_0 = F$  as desired This Proves

(i)  $\Rightarrow$  (ii) & (ii)  $\Rightarrow$  (i) As explained earlier,

$E = F(\alpha)$  for some  $\alpha \in E$ , let

$G(E/F) = \{\sigma_1 = \text{identity}, \sigma_2, \dots, \sigma_n\}$  Consider

the polynomial  $P(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \dots (x - \sigma_n(\alpha))$

Now each  $\sigma_i \in G(E/F)$  induces a natural homomorphism.

$$\sigma_i^*: E[x] \rightarrow E[x]$$

where

$$\sigma_i^*(a_0 + a_1x + \dots + a_nx^n) = \sigma_i(a_0) + \sigma_i(a_1)x + \dots + \sigma_i(a_n)x^n$$

So ...

$$\sigma_i^*(P(x)) = (x - (\sigma_i \sigma_1)(\alpha))(x - (\sigma_i \sigma_2)(\alpha)) \dots (x - (\sigma_i \sigma_n)(\alpha))$$

But since  $\sigma_1, \sigma_2, \dots, \sigma_n$  are distinct members of  $G(E/F)$ , these  $F$ -automorphisms are only a permutation of  $\sigma_1, \sigma_2, \dots, \sigma_n$ . Hence

$\sigma_i^*(P(x)) = P(x)$  for all  $i = 1, 2, \dots, n$  Now by expanding  $P(x)$  we have

$$P(x) = x^n - c_1x^{n-1} + c_2x^{n-2} + \dots + (-1)^n c_n$$

where  $c_i \in E$ . Therefore  $\sigma_i^*(P(x)) = P(x)$  implies

$$\sigma_i(c_j) = c_j \quad \text{for } i, j = 1, 2, \dots, n$$

This gives that  $c_j$  is in the fixed field of  $G(E/F)$

So by hypothesis,  $c_j \in F$ ,  $j = 1, \dots, n$ . Hence

$P(x) \in F[x]$ . Also, all the roots of  $P(x)$  lie in  $E$ .

because  $E = F(\alpha)$  and  $\alpha$  is one of the roots of  $f(x)$ .  
 $E$  is a splitting field of  $f(x) \in F[x]$ . This proves (i)  $\rightarrow$  (ii)

(ii)  $\rightarrow$  (iii) from Theorem [1.5]

(iii)  $\rightarrow$  (ii) By equation (2)  $[E:E_0] = |G(E/F)|$ . Thus  
by (iii) we get  $[E:E_0] = [E:F]$ . Hence  $E_0 = F$ ,  
proving (iii)  $\rightarrow$  (ii). This completes the proof.

examples - A - The group  $G(\mathbb{Q}(\alpha)/\mathbb{Q})$ , where  
 $\alpha^5 = 1$  and  $\alpha \neq 1$ , is isomorphic to the  
cyclic group of order 4.

Solution 8-

===== // clearly  $\alpha^5 - 1 = (\alpha - 1)(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4)$   
so  $\alpha$  is a root of a polynomial  $P(x) = 1 + x + x^2$   
 $+ x^3 + x^4 \in \mathbb{Q}[x]$  because  $P(x)$  is irreducible  
over  $\mathbb{Q}$ ,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ . The roots of  $x^5 - 1$   
are  $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ . So  $\mathbb{Q}(\alpha)$  is the splitting  
field of  $x^5 - 1 \in \mathbb{Q}[x]$  and hence a normal  
extension of  $\mathbb{Q}$ . Thus,

$$|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$$

because  $\{1, \alpha, \alpha^2, \alpha^3\}$  is a basis of  $\mathbb{Q}(\alpha)$  over  
 $\mathbb{Q}$ , a typical element of  $\mathbb{Q}(\alpha)$  is

$$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3, \quad a_i \in \mathbb{Q}$$

-The four  $\mathbb{Q}$ -automorphisms of  $\mathbb{Q}(\alpha)$  are  
indeed the following

$$\sigma_1: a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \rightarrow a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$$

$$\sigma_2: a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \rightarrow a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha^8 \\ = a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha^2$$

$$\sigma_3: a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \rightarrow a_0 + a_1\alpha^3 + a_2\alpha^6 + a_3\alpha^9 \\ = a_0 + a_1\alpha^3 + a_2\alpha + a_3\alpha^4$$

$$\sigma_4: a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \rightarrow a_0 + a_1\alpha^4 + a_2\alpha^8 + a_3\alpha^{12} \\ = a_0 + a_1\alpha^4 + a_2\alpha^3 + a_3\alpha^2$$

these from the cyclic group of order 4 generated by  $\sigma_2$  or  $\sigma_3$ .

example let  $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$  where  $\omega^3 = 1, \omega \neq 1$

let  $\sigma_1$  be the identity automorphism of  $E$ ,

and let  $\sigma_2$  be an automorphism of  $E$

such that  $\sigma_2 = \omega^2$  and  $\sigma_2(\sqrt[3]{2}) = \omega(\sqrt[3]{2})$  if

$G = \{\sigma_1, \sigma_2\}$  then  $E_G = \mathbb{Q}(\sqrt[3]{2}, \omega^2)$

Solution

now  $\alpha \in E_G$  if and only if

$\sigma_2(\alpha) = \alpha$  consider the following diagram of towers of fields:

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \omega) \\ | \text{ basis } (1, \omega) \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \text{ basis } \{1, \sqrt[3]{2}, \sqrt[3]{4}\} \\ \mathbb{Q} \end{array}$$

Thus,  $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$  is a basis of

$\mathbb{Q}(\sqrt[3]{2}, \omega)$  over  $\mathbb{Q}$ , so let

$$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{4}$$

be an element in  $\mathbb{Q}(\sqrt[3]{2}, \omega)$  then

$$\sigma_2(\alpha) = a + b\sqrt[3]{2}w + c w^2\sqrt[3]{4} + d w^2 + e w^2 w\sqrt[3]{2} + f w^2 w^2\sqrt[3]{4}$$

$$= a + b w\sqrt[3]{2} + c(-1-w)\sqrt[3]{4} + d(-1-w) + e\sqrt[3]{2} + f w\sqrt[3]{4}$$

$$= (a-d) + e\sqrt[3]{2} - c\sqrt[3]{4} - dw + b w\sqrt[3]{2} - (c-f)w\sqrt[3]{4}$$

So  $\rightarrow \sigma_2(\alpha) = \alpha$  implies  $a = a-d, b = e, c = -c$

$$d = -d, e = b \text{ and } f = -c + b$$

So we obtained  $d = 0 = c, b = e$  and  $f, a$  arbitrary, Thus

$$\alpha = a + b\sqrt[3]{2}(1+w) + f w\sqrt[3]{4}$$

$$= a - b w^2\sqrt[3]{2} + f w\sqrt[3]{4}$$

$$= a - b w^2\sqrt[3]{2} + f (w^2\sqrt[3]{2})^2 \text{ there for } E_G = \mathbb{Q}(w^2\sqrt[3]{2})$$

#### 1.4 Fundamental theorem of Galois theory

we are now ready to prove the Fundamental theorem of Galois theory. First we give a couple of definitions.

Definition <sup>(1)</sup> let  $f(x) \in F[x]$  be a polynomial and let  $K$  be its splitting field over  $F$ . Then the group  $G(K/F)$  of  $F$ -automorphisms of  $K$  is called Galois group of  $f(x)$  over  $F$ .

Definition <sup>(2)</sup> A finite, normal and separable extension  $E$  of a field  $F$  is called a Galois extension  $E$  of  $F$  for example, if  $f(x) \in F[x]$  is a polynomial over a field  $F$  of characteristic zero, then its splitting field  $E$  over  $F$  is a Galois extension of  $F$ .

## Theorem (Fundamental theorem of Galois theory)

Let  $E$  be a Galois extension of  $F$ . Let  $K$  be any subfield of  $E$  containing  $F$ . Then mapping  $K \rightarrow G(E/K)$  sets up onto one correspondence from the set of subfields of  $E$  containing  $F$  to the subgroups of  $G(E/F)$  such that:

- 1-  $K = E_{G(E/K)}$
- 2- For any subgroup  $H$  of  $G(E/F)$ ,  $H = G(E/E_H)$
- 3-  $[E:K] = |G(E/K)|$ ,  $[K:F] = \text{index of } G(E/K) \text{ in } G(E/F)$
- 4-  $K$  is a normal extension of  $F$  if and only if  $G(E/K)$  is a normal subgroup of  $G(E/F)$ .
- 5- If  $K$  is a normal extension of  $F$ , then  $G(K/F) \cong G(E/F) / G(E/K)$

### example

the Galois group of  $x^4 - 2 \in \mathbb{Q}[x]$  is the octic group (= group of symmetries of a square)

Solution

$x^4 - 2$  is irreducible over  $\mathbb{Q}$  and  $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) \in \mathbb{Q}(\sqrt[4]{2}, i)[x]$ . Therefore  $E = \mathbb{Q}(\sqrt[4]{2}, i)$  is the splitting field of  $x^4 - 2$  over  $\mathbb{Q}$

$[E:\mathbb{Q}] = 8$  Also  $E$  is a normal separable extension of  $\mathbb{Q}$ . This gives  $|G(E/\mathbb{Q})| = [E:\mathbb{Q}] = 8$ . If  $\sigma \in G(E/\mathbb{Q})$  and  $B \in E$ ; then

$$B = a_0 + a_1 \sqrt[4]{2} + a_2 (\sqrt[4]{2})^2 + a_3 (\sqrt[4]{2})^3 + a_4 (i) + a_5 (i\sqrt[4]{2}) + a_6 (i(\sqrt[4]{2})^2) + a_7 (i(\sqrt[4]{2})^3)$$

So we have

$$\begin{aligned} \sigma(B) &= a_0 + a_1 \sigma(\sqrt[4]{2}) + a_2 \sigma(\sqrt[4]{2})^2 + a_3 \sigma(\sqrt[4]{2})^3 \\ &\quad + a_4 \sigma(i) + a_5 \sigma(i) \sigma(\sqrt[4]{2}) + a_6 \sigma(i) \sigma(\sqrt[4]{2})^2 \\ &\quad + a_7 \sigma(i) \sigma(\sqrt[4]{2})^3 \end{aligned}$$

Therefore  $\sigma$  is determined by its effect on  $i$  and on  $\sqrt[4]{2}$ . Because  $\sigma(i)$  must be  $i$  or  $-i$  because  $\sigma(\sqrt[4]{2})$  must be  $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}$  or  $-i\sqrt[4]{2}$  and because there are eight elements in  $G(E/\mathbb{Q})$ , it follows that  $G(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_8\}$ , where

$$\sigma_1: \begin{matrix} \sqrt[4]{2} \rightarrow \sqrt[4]{2} \\ i \rightarrow i \end{matrix}$$

$$\sigma_2: \begin{matrix} \sqrt[4]{2} \rightarrow -\sqrt[4]{2} \\ i \rightarrow i \end{matrix}$$

$$\sigma_3: \begin{matrix} \sqrt[4]{2} \rightarrow \sqrt[4]{2} \\ i \rightarrow -i \end{matrix}$$

$$\sigma_4: \begin{matrix} \sqrt[4]{2} \rightarrow -\sqrt[4]{2} \\ i \rightarrow -i \end{matrix}$$

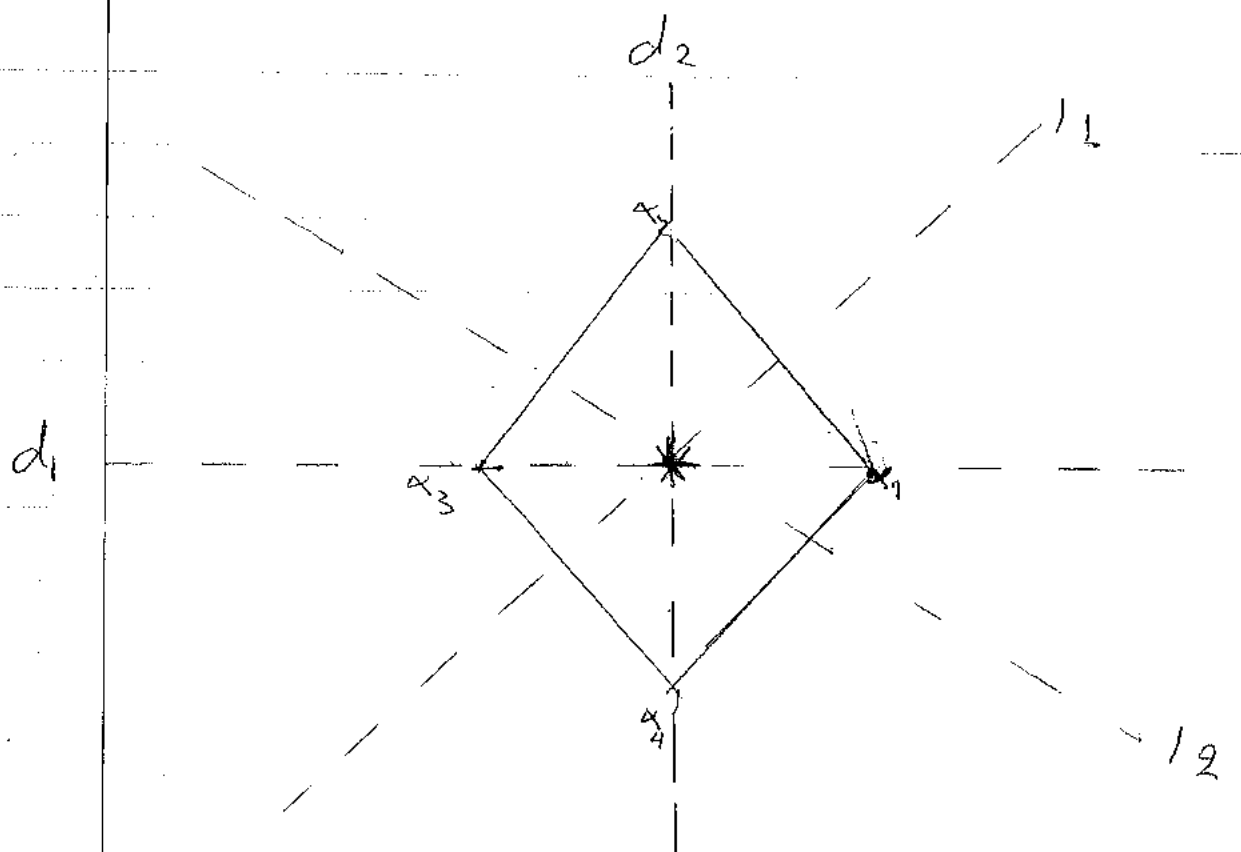
$$\sigma_5: \begin{matrix} \sqrt[4]{2} \rightarrow i\sqrt[4]{2} \\ i \rightarrow i \end{matrix}$$

$$\sigma_6: \begin{matrix} \sqrt[4]{2} \rightarrow -i\sqrt[4]{2} \\ i \rightarrow i \end{matrix}$$

$$\sigma_7: \begin{matrix} \sqrt[4]{2} \rightarrow i\sqrt[4]{2} \\ i \rightarrow -i \end{matrix}$$

$$\sigma_8: \begin{matrix} \sqrt[4]{2} \rightarrow -i\sqrt[4]{2} \\ i \rightarrow -i \end{matrix}$$

$$\text{let } \alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$$



Then the elements of  $G(E/\mathbb{Q})$  permute the roots  $\alpha_1, \alpha_2, \alpha_3$  and  $\alpha_4$  of  $A_4 - 2$  as follows (See the diagram):

$\sigma_1$  :  $0^\circ$  rotation

$\sigma_5$  : reflection about  $d_1$

$\sigma_2$  :  $90^\circ$  rotation

$\sigma_6$  : reflection about  $l_1$

$\sigma_3$  :  $180^\circ$  rotation

$\sigma_7$  : reflection about  $d_2$

$\sigma_4$  :  $270^\circ$  rotation

$\sigma_8$  : reflection about  $l_2$

## Example 2

I illustrate the 1-1 correspondence between subgroups and subfield by using the Galois group of  $x^4 - 2 \in \mathbb{Q}[x]$ .

Solution We saw in the solution to example (1) that  $E = \mathbb{Q}(\sqrt[4]{2}, i)$  is the splitting field of  $x^4 - 2$  over  $\mathbb{Q}$  and that the Galois group  $G$  of  $x^4 - 2$  is the Galois group in the solution of that problem.  $G$  is the identity automorphism  $E$ . Set  $\sigma_2 = \sigma$  then  $\sigma_3 = \sigma^2, \sigma_4 = \sigma^3$ , and  $\sigma^4 = E$ . Next set  $\sigma_5 = \tau$  then  $\tau^2 = E, \sigma\tau = \tau\sigma, \tau\sigma^2 = \sigma^2\tau$  and  $\tau\sigma^3 = \sigma^3\tau$ . Finally we have  $\tau\sigma = \sigma^3\tau$ .

The group  $G$  has four normal subgroups other than itself and the identity subgroup:

$$N_1 = \{E, \sigma\tau, \sigma^2, \sigma^3, \tau\}$$

$$N_2 = \{E, \sigma, \sigma^2, \sigma^3\}$$

$$N_3 = \{E, \tau, \sigma^2, \sigma^3, \tau\} \text{ and}$$

$$N_4 = \{E, \sigma^2\}$$

and four nonnormal subgroups:

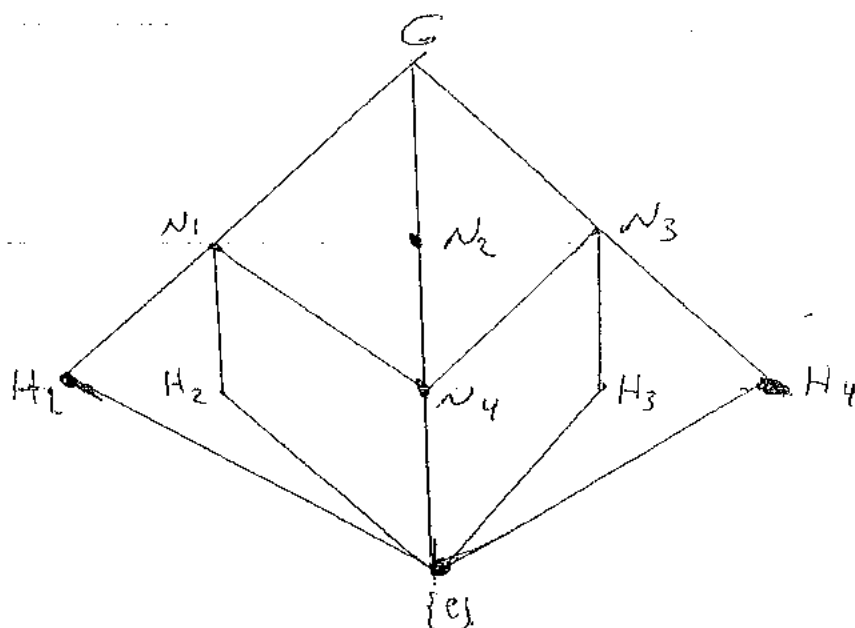
$$H_1 = \{E, \sigma^3, \tau\}$$

$$H_2 = \{E, \sigma\tau\}$$

$$H_3 = \{E, \sigma^2\tau\} \text{ and}$$

$$H_4 = \{E, \tau\}$$

The inclusion relations between these subgroups are shown in the following diagram:



— we now describe the fixed fields under these subgroups. we begin with  $E_{N_4}$ , the fixed field of the subgroup  $N_4$ . let  $\alpha = \sqrt[4]{2}$  and let

$$x = a_1 + a_2\alpha + a_3\alpha^2 + a_4\alpha^3 + a_5i + a_6i\alpha + a_7i\alpha^2 + a_8i\alpha^3$$

by any elements of  $\mathbb{Q}(\alpha, i)$ . Then  $x \in E_{N_4}$  iff  $x = \sigma^2(x)$  because  $\sigma(\alpha) = i\alpha$  and  $\sigma(i) = i$ , we have

$$\sigma(x) = a_1 + a_2i\alpha + a_3\alpha^2 - a_4i\alpha^3 + a_5i - a_6\alpha - a_7i\alpha^2 + a_8\alpha^3$$

$$= a_1 - a_6\alpha - a_3\alpha^2 + a_8\alpha^3 + a_5i + a_2i\alpha - a_7i\alpha^2 - a_4i\alpha^3$$

$$\sigma^2(x) = a_1 - a_2\alpha + a_3\alpha^2 - a_4\alpha^3 + a_5i - a_6i\alpha + a_7i\alpha^2 - a_8i\alpha^3$$

#

Hence  $x = \sigma^2(x)$  if and only if  $a_2 = -a_2$

$$a_4 = -a_4, \quad a_6 = -a_6, \quad a_8 = -a_8 \text{ So}$$

$a_2 = a_4 = a_6 = a_8 = 0$  and  $a_1, a_3, a_5$  and  $a_7$  are arbitrary therefore,

$$x = a_1 + a_3 x^2 + a_5 i + a_7 i x^2$$

Thus,  $E_{N_4} = \mathbb{Q}(\sqrt{2}, i)$

Next, to find  $E_{N_3}$ , we note that  $x \in E_{N_3}$  iff

$$x = \tau(x) = \sigma^2(x) = \sigma^2 \tau(x)$$

Let

$$x = a_1 + a_2 x + a_3 x^2 + a_4 x^3 + a_5 i + a_6 i x + a_7 i x^2 + a_8 i x^3$$

because  $x = \sigma^2(x)$  implies  $a_2 = a_4 = a_6 = a_8 = 0$   
we have:-

$$x = a_1 + a_3 x^2 + a_5 i + a_7 i x^2.$$

Further  $\tau(x) = x$  and  $\tau(i) = -i$  So

$$\tau(x) = a_1 + a_3 x^2 - a_5 i - a_7 i x^2$$

Therefore

$x = \tau(x)$  implies  $a_5 = 0 = a_7$ , yielding

$$x = \tau(x) = a_1 + a_3 x^2$$

Applying  $\sigma^2$  we obtain

$$\sigma^2 \tau(x) = a_1 + a_3 x^2,$$

Since  $\sigma(x) = x$  This Proves  $x \in E_{N_3}$  iff  $x = a_1 + a_3 x^2$ ,

where  $a_1$  and  $a_3$  are arbitrary. Thus  $E_{N_3} = \mathbb{Q}(\sqrt{2})$

Similarly,  $E_{N_1} = \mathbb{Q}(i, \sqrt{2})$  and  $E_{N_2} = \mathbb{Q}(i) \cdot E_{N_4}$

$E_{N_3}$ ,  $E_{N_2}$  and  $E_{N_1}$  are normal extensions of  $\mathbb{Q}$  - being splitting fields of Polynomials  $(x^2+1)$ ,  $(x^2-2)$ ,  $(x^2-2)$ ,  $(x^2+1)$ , and  $(x^2+2)$  respectively

similar computations show that  $E_{H_1} = \mathbb{Q}(1-i)x$ ,  
 $E_{H_2} = \mathbb{Q}(1+i)x$ ,  $E_{H_3} = \mathbb{Q}(ix)$  and  $E_{H_4} = \mathbb{Q}(x)$

### 1.5 Theorem (Fundamental theorem of algebra)

Every polynomial  $P(x) \in \mathbb{C}[x]$  factors into linear factors in  $\mathbb{C}[x]$

Proof

Let  $P(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{C}[x]$   
 let  $g(x) = (x^2+1)(a_0 + a_1x + \dots + a_nx^n)(\bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n)$

Then  $g(x) \in \mathbb{R}[x]$  let  $E$  be the splitting field of  $g(x)$  over  $\mathbb{R}$  then  $\mathbb{R} \subset \mathbb{C} \subset E$  we prove  $E = \mathbb{C}$

First we assert that there does not exist a subfield  $K$  of  $E$  containing  $\mathbb{C}$  such that  $[K:\mathbb{C}] = 2$ . Suppose such a subfield exists. because  $K$  is finite separable extension of  $\mathbb{C}$   $K = \mathbb{C}(x)$  for some  $x \in K$ , if  $P(x) \in \mathbb{C}[x]$  is the minimal polynomial of  $x$  over  $\mathbb{C}$ , then  $\deg P(x) = 2$ . Suppose

$P(x) = x^2 + 2ax + b$ . Then

$$P(x) = (x+a)^2 - (a^2 - b) = (x+a - \sqrt{a^2 - b})(x+a + \sqrt{a^2 - b})$$

which is a contradiction because  $P(x)$  is irreducible over  $\mathbb{C}$  (observe that if  $c \in \mathbb{C}$  then  $\sqrt{c} \in \mathbb{C}$ ).

This proves our assertion.

Let  $G = G(E/\mathbb{R})$  be the Galois group of  $g(x)$  over  $\mathbb{R}$ .

let  $|G| = 2^m q$ , where  $q$  is an odd integer. 19

Let  $H$  be the 2-sylow subgroup of  $G$  and let  $L$  be the corresponding subfield of  $E$ . We exhibit the foregoing considerations in the following diagram:

$$E \longleftrightarrow \{e\}$$

$$L \longleftrightarrow H$$

$$C \longleftrightarrow G(E/C)$$

$$R \longleftrightarrow G(E/R)$$

Then  $[E:L] = 2^m$ , so  $[L:R] = q$ . Also because  $L$  is a finite separable extension of  $R$ ,  $L = R(B)$  for some  $B \in L$ . Thus, the minimal polynomial

$$q(x) = b_0 + b_1x + \dots + b_q x^q \in R[x]$$

of  $B$  is of odd degree  $q$  but this is impossible unless  $q=1$  because by the intermediate value theorem in calculus every equation of odd degree over the reals has a real root. Hence  $q=1$ , so

$$[E:R] = 2^m \text{ This implies that } [E:C] = 2^{m-1} \text{ Then}$$

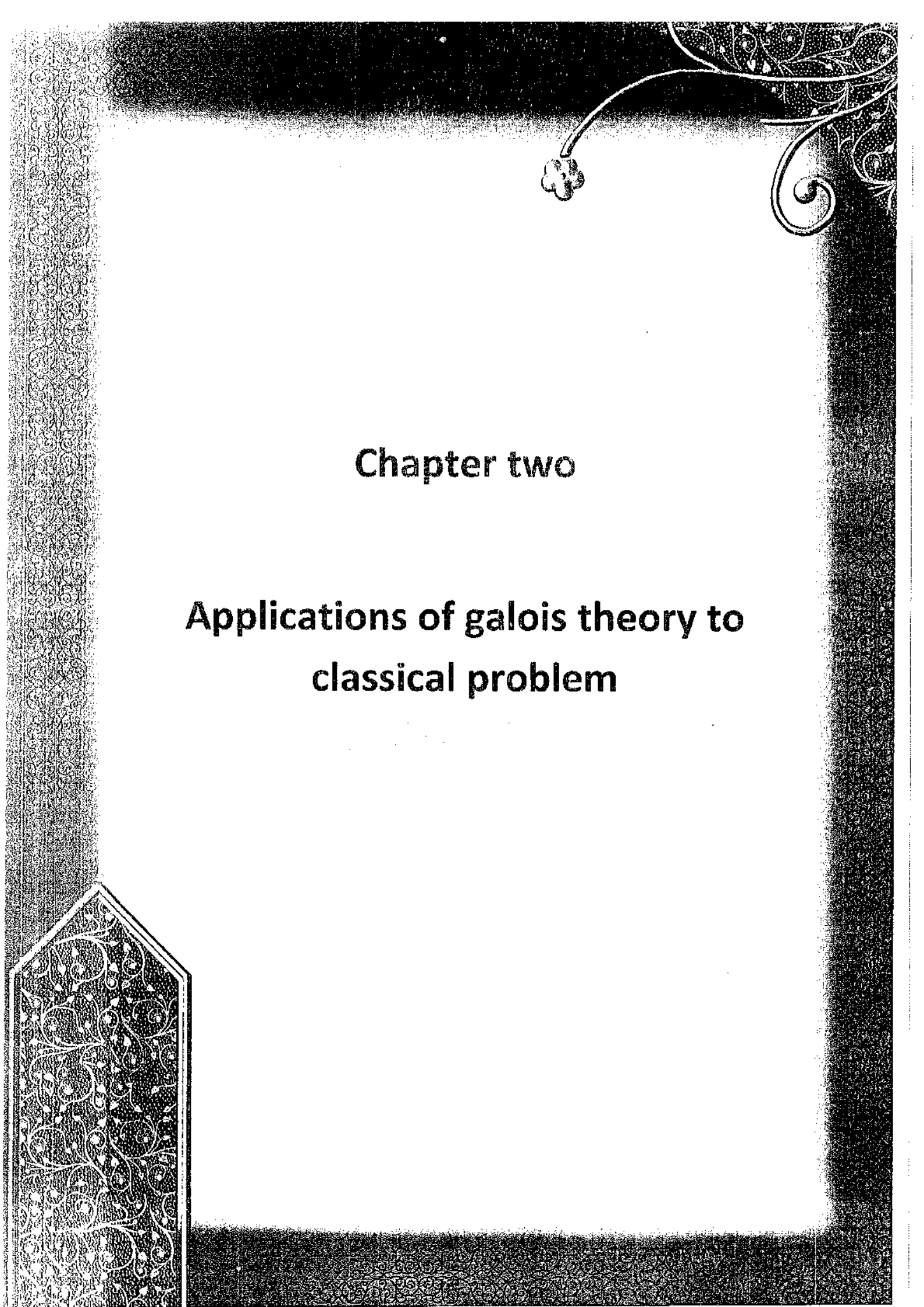
the subgroup  $G(E/C)$  of order  $2^{m-2}$ , and

if  $m > 1$  let  $H'$  be subgroup of  $G(E/C)$  of order  $2^{m-2}$ , and let  $L'$  be the corresponding subfield of  $E$  clearly,  $L' \supseteq C$ . Then  $[E:L'] = 2^{m-2}$

So  $[L':C] = 2$  a contradiction of the assertion

proved in the beginning, hence  $m=1$  Then

$[E:R] = 2$  with  $E \supseteq C$  implies  $E = C$ , as claimed.



## Chapter two

# Applications of galois theory to classical problem

## Chapter 20:-

### 2-1 Application of Galois theory to classical Problem 1 - Roots of unity and cyclotomic polynomials.

#### Definition

\* Let  $E$  be a field, and let  $n$  be a positive integer.

An element  $\omega \in E$  is called a primitive  $n$ th root of unity if  $\omega^n = 1$  but  $\omega^m \neq 1$  for any positive integer  $m < n$ .

\* Note that the complex numbers satisfying  $x^n = 1$  form a finite sub-group  $H$  of the multiplicative group of the non zero elements of the field  $\mathbb{C}$  of complex numbers. Also  $H$  is a cyclic group generated by any primitive  $n$ th root  $\omega$  of unity. There are exactly  $\phi(n)$  primitive  $n$ th roots of unity for each positive integer  $n$ .

\* These are  $\cos(2k\pi/n) + i \sin(2k\pi/n)$  where  $k$  is a positive integer less than  $n$  and prime to  $n$ .

## Theorem

Let  $F$  be a field and let  $U$  be a finite

sub group of the multiplicative group

$F^* = F - \{0\}$  then  $U$  is cyclic. In particular

the roots of  $x^n - 1 \in F[x]$  form a cyclic group

## Proof

Let  $f(x) = x^n - 1$  and let  $P_1, \dots, P_k$  be the distinct primes dividing  $n$ . Then  $|S(P_i)| = P_i^{r_i}$  and  $P_1, \dots, P_k$  are distinct

Primes. We proceed to show that each  $S(P_i)$  is cyclic. Let  $a \in S(P_i)$  be such

that  $o(a)$  is max (max = say  $P_i^{s_i}$ ). Because  $o(a) \mid P_i^{r_i}$ , we have  $s_i \leq r_i$ . Further, for

each  $x \in S(P_i)$ ,  $o(x) \mid P_i^{r_i} = P_i^{s_i}$ . Therefore,  $x^{P_i^{s_i}} = 1$  implies  $x^{P_i^{s_i}} = 1$ . Hence, for

all  $x \in S(P_i)$ ,  $x^{P_i^{s_i}} = 1$  because the equation  $x^{P_i^{s_i}} = 1$  has at most  $P_i^{s_i}$  roots, it follows

that  $P_i^{s_i} \geq P_i^{r_i}$ . But this yields  $s_i = r_i$  since

$P_i^{\alpha} = P_i^{\alpha i}$  therefore,  $O(\alpha) = P_i^n = |S(P_i)|$ , and hence  $S(P_i)$  is a cyclic group generated by

$\alpha$ . we also know that if  $A$  and  $B$  are cyclic groups of orders  $m$  and  $n$  respectively

with  $(m, n) = 1$  then  $A \times B$  is again cyclic. Hence,  $G$  is cyclic.

Theorem 9  
~~Let  $F$  be a field and let  $n$  be a positive integer. Then there exists a primitive  $n$ th root of unity in some extension  $E$  of  $F$  if and only if either  $\text{char } F = 0$  or  $\text{char } F \nmid n$ .~~

Let  $F$  be a field and let  $n$  be a positive integer. Then there exists a primitive  $n$ th root of unity in some extension  $E$  of  $F$  if and only if either  $\text{char } F = 0$  or  $\text{char } F \nmid n$ .

Proof

Let  $F(x) = x^n - 1 \in F[x]$ , and let  $\text{char } F = 0$  or  $\text{char } F \nmid n$ . Then  $F'(x) = nx^{n-1} \neq 0$ . Thus,  $F(x)$  has  $n$  distinct roots (in its splitting field  $E$  over  $F$ ), and they clearly form a group, say  $H$ . So by the theorem this group  $H$ , consisting of  $n$  distinct roots of  $x^n - 1$ , is a cyclic group. Now if  $\omega \in H$  is a generator of  $H$

then  $\omega^n = 1$  but  $\omega^m \neq 1$  for any positive integer  $m < n$ . Hence  $\omega$  is a primitive  $n$ th

root of unity. In an extension field  $E$  of  $F$  conversely let  $\omega$  be a primitive  $n$ th root of

unity in some extension field  $E$  of  $F$ . Then  $\omega, \omega^2, \dots, \omega^{n-1}$  are clearly  $n$  distinct roots of  $f(x) = x^n - 1$ . So  $f(x)$  does not possess multiple roots

But then  $f'(x) = nx^{n-1} \neq 0$ . This implies either  $\text{char } F = 0$  or  $\text{char } F \nmid n$ .

## 2-2 Definition

Let  $n$  be a positive integer, and let  $F$  be a field of characteristic zero or characteristic  $p \nmid n$ .

Then the polynomial  $\Phi_n(x) = \prod_{\omega} (x - \omega)$  where the product runs over all the primitive  $n$ th roots

$\omega$  of unity (i.e. the primitive  $n$ th root of  $x^n - 1$  over  $F$ ) is called the  $n$ th cyclotomic polynomial.

For example //  $\Phi_1(x) = x - 1$ ,  $\Phi_2(x) = x + 1$ ,  $\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$ ,  $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = x^2 - x + 1$

## Theorem //

~~Let~~  $f_n(x) = x^n - 1$  over  $\mathbb{Q}$

Let  $\omega$  be a primitive  $n$ th root of unity in  $\mathbb{C}$ . Then

$\mathbb{Q}(\omega)$  is the splitting field of  $\Phi(n)$  in  $\mathbb{Z}[x]$ .

~~Proof //~~

Let  $\omega$  be a primitive  $n$ th root of unity in  $\mathbb{C}$ . Then  $\mathbb{Q}(\omega)$  is the splitting field of  $\Phi_n(x)$  and also of  $x^n - 1 \in \mathbb{Q}[x]$ . Further  $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n) = |G(\mathbb{Q}(\omega)/\mathbb{Q})|$  and  $G(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ , the multiplicative group formed by the units of  $\mathbb{Z}/n\mathbb{Z}$ .

~~Remark //~~

— If  $p$  is an odd prime, then  $(\mathbb{Z}/(p^e))^*$  the multiplicative group formed by the units of the ring  $\mathbb{Z}/(p^e)$  is cyclic. The proof of this result is quite technical. The interested reader may find the proof in any advanced text. For  $p=2$  the following example shows that the result is not necessarily true.

## Example //

The Galois group of  $x^4 + x^2 + 1$  is the same as that of  $x^6 - 1$  and is of order 2.

Solution //

Note  $x^4 + x^2 + 1 = z^2 + z + 1$  where  $z = x^2$  But

$z^2 + z + 1$  is the minimal polynomial for a

Primitive third root of unity. So the splitting

Field of  $x^4 + x^2 + 1$  will contain the square roots

of  $e^{\frac{2\pi i}{3}}$  and  $e^{\frac{4\pi i}{3}}$ . Thus we need to adjoin

$$e^{\frac{\pi i}{3}} = \left( e^{\frac{2\pi i}{3}} \right)^{\frac{1}{2}} \Rightarrow e^{\frac{4\pi i}{3}} = - \left( e^{\frac{\pi i}{3}} \right)^{\frac{1}{2}}$$

$$e^{\frac{2\pi i}{3}} = \left( e^{\frac{4\pi i}{3}} \right)^{\frac{1}{2}}$$

So  $E = \mathbb{Q}(\alpha)$  where  $\alpha = e^{\frac{\pi i}{3}}$  is the splitting

Field of  $x^4 + x^2 + 1 \in \mathbb{Q}[x]$  because  $\alpha$  is a Primitive

sixth root of unity.  $E$  is the splitting Field

of  $x^6 - 1$ .

then

$G(E/\mathbb{Q}) = (\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\}$  is the group of order 2.

## # cyclic extensions 2-3

Definition let  $E$  be a Galois extension of  $F$

Then  $E$  is called a cyclic extension of  $F$  if

$G(E/F)$  is a cyclic group.

Example of cyclic extensions ~

a) if  $\omega$  is a primitive  $p$ th root of unity and

$E = \mathbb{Q}(\omega)$  is the splitting field of  $x^p - 1 \in \mathbb{Q}[x]$

then  $E$  is a Galois extension of  $\mathbb{Q}$  because

$x^p - 1$  is a separable polynomial. Also  $E$  is a

cyclic extension.

(b) All finite extensions of finite fields are

separable. Thus the splitting field  $E$  of a

polynomial  $f(x)$  over a finite field  $F$  is a

Galois extension. Furthermore  $G(E/F)$

is cyclic. Therefore all splitting fields

over finite fields are cyclic extensions.

### Proposition

Let  $F$  be a field of nonzero characteristic  $p$ . Then for every positive integer  $k$  the mapping  $\pi_k$  of  $F$  into itself, defined by  $\pi_k(x) = x^{p^k}$  for all elements  $x$  of  $F$ , is an embedding of  $F$  into itself. (The mapping  $\pi_1(x) = x^p$  is called the Frobenius endomorphism.)

### Lemma

Let  $E$  be a finite extension of  $F$ . Suppose

$$f: G \rightarrow E^*, \quad E^* = E - \{0\} \quad \text{has the property}$$

$$\text{that } f(\sigma\eta) = \sigma(f(\eta)) f(\sigma) \quad \text{for all } \sigma, \eta \in G$$

Then there exist  $\alpha \in E^*$

such that  $\alpha \in E^*$  such that  $f(\sigma) = \sigma(\alpha^{-1}) \alpha$  for

all  $\sigma \in G$  (The mapping  $f$  in the hypothesis

of the lemma is called a crossed homomorphism

PROOF //

For all  $\eta \in G$ ,  $f(\eta) \in E^*$ , so

$f(\eta) \neq 0$  Thus if  $\sum_{\eta \in G} f(\eta) \eta(b) = 0$

for all  $b \in E^*$ , then by

$f(\eta) = 0$ , which is not true, Hence, there

exists  $b \in E^*$  such that  $\sum_{\eta \in G} f(\eta) \eta(b) = \alpha \neq 0$

Then for any  $\sigma \in G$ , we get

$$\sum_{\eta \in G} \sigma(f(\eta)) \eta(b) = \sigma(\alpha)$$

which give:-

$$\sum_{\eta \in G} \sigma(f(\eta)) \sigma(\eta(b)) = \sigma(\alpha)$$

Thus, by using  $\sigma(f(\eta)) = (f(\sigma))^{-1} f(\sigma\eta)$  we

have

$$\sum_{\eta \in G} (f(\sigma))^{-1} f(\sigma\eta) \eta(b) = \sigma(\alpha)$$

$$\text{But } \rightarrow (\sigma\eta | \eta \in G) = (\eta | \eta \in G)$$

$$\text{Hence } (f(\sigma))^{-1} \sum_{\eta \in G} f(\eta) \eta(b) = \sigma(\alpha)$$

This implies

$$(f(\sigma))^{-1} \alpha = \sigma(\alpha) \rightarrow \text{Equivalently, we get } \alpha \sigma(\alpha^{-1}) = f(\sigma)$$

This completes the Proof.

| Contents                                | Pages     |
|-----------------------------------------|-----------|
| <b>Chapter one</b>                      | <b>1</b>  |
| 1-1 theorem                             | 2         |
| 1-2 lemma dedekind                      | 3         |
| 1-3 theorem                             | 8         |
| 1-4 fundametal theorem of galois theory | 12        |
| 1-5 fundamental theorem of algebra      | 19        |
| <b>Chapter two</b>                      | <b>21</b> |
| 2-1 application of galois theory        | 21        |
| 2-2 deffinition                         | 24        |
| 2-3 cyclic extensions                   | 27        |

## Selected bibliography

1\_ Artin M.algebra prentice-hall.  
Englewood cliffs N.J..1991

2 \_ Zariski. O. and Samuel. P..  
Comnutative Algebra.I, van  
Nostrand, New yor;

3\_ Galois theory

Emil Artin, Arthur Norton Milgram

4\_ Fields and Galois Theory

j.S.Milne

## ... Abstract ...

Galois used Permutation groups to describe how the various roots of a given Polynomial equation are related to each other the modern approach to Galois theory developed by Richard Dedekind, Leopold Kronecker among others, involves studying automorphisms of field extensions. Further abstraction of Galois theory is achieved by the theory of Galois connections. Application to classical problems.