

# An isomorphism  $\sigma$  of  $K$  with itself is called an automorphism of  $K$ .

# The collection of automorphisms of  $K$  is denoted by  $\text{Aut}(K)$ .

$$\text{Aut}(K) = \{ f: K \rightarrow K \mid f \text{ is an isomorphism} \}$$

$$= \{ \sigma: K \rightarrow K \mid \sigma \text{ is an isomorphism} \}$$

$\Rightarrow$  \* An automorphism  $\sigma \in \text{Aut}(K)$  is said to fix an element  $\alpha \in K$

if  $\sigma(\alpha) = \alpha$ .

\* If  $F$  is a subset (subfield) of  $K$ , then an automorphism  $\sigma$  is said to fix  $F$  if it fixes all the elements of  $F$ .  
 $\sigma a = a$  for all  $a \in F$ .

$\Rightarrow$  The prime field of  $K$  is generated by  $1 \in K$ .

Since any automorphism  $\sigma$  takes  $1$  to  $1$  (and  $0$  to  $0$ )  
 i.e.  $\sigma(1) = 1$ .

$\sigma(a) = a$  for all  $a$  in the prime field.

Automorphism of a field  $K$  fixes

its prime subfield.

Example:

Take  $K = \mathbb{Q}$ ,  $\text{Aut}(\mathbb{Q})$  is trivial.

Take an automorphism

$$\sigma: \mathbb{Q} \rightarrow \mathbb{Q}$$

Suppose  $\frac{p}{q} \in \mathbb{Q}^*$  with  $p, q \in \mathbb{N}$ .

$$\text{Then } \sigma\left(\frac{p}{q}\right) = \frac{\sigma(p)}{\sigma(q)}$$

$$= \frac{\overbrace{\sigma(1 + \dots + 1)}^{p \text{ times}}}{\underbrace{\sigma(1 + \dots + 1)}_{q \text{ times}}}$$

$$= \frac{\overbrace{\sigma(1) + \sigma(1) + \dots + \sigma(1)}^{p \text{ times}}}{\underbrace{\sigma(1) + \sigma(1) + \dots + \sigma(1)}_{q \text{ times}}}$$

$$= \frac{p}{q}$$

Since  $\sigma(1) = 1$ .

$$\text{i.e. } \sigma\left(\frac{p}{q}\right) = \frac{p}{q}$$

Let  $K/F$  be an extension of fields. Then  
~~Let  $A$~~   $\text{Aut}(K/F)$  be the collection  
of automorphisms of  $K$  which fix  $F$ .

#  $\text{Aut}(K)$  is group.

Take  $\sigma, \tau \in \text{Aut}(K)$

$$(\sigma \circ \tau)(xy) = \sigma(\tau(xy)) \\ = \sigma(\tau(x)\tau(y))$$

$$= \sigma(\tau(x))\sigma(\tau(y))$$

$$= (\sigma \circ \tau)(x)(\sigma \circ \tau)(y)$$

for all  $x, y \in K$ .

$\Rightarrow \sigma \circ \tau$  is a group homomorphism.

~~$\sigma \circ \text{Id}_K = \text{Id}_K \circ \sigma$~~

$$\Rightarrow \sigma \circ \text{Id}_K = \text{Id}_K \circ \sigma$$

where  $\text{Id}_K = \text{identity}$

$$\Rightarrow \sigma \circ \sigma^{-1} = \text{Id}_K$$

$$\Rightarrow \sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$$

every all group properties.

Suppose that  $K/\mathbb{F}$  be an extension of fields. Then an automorphism of  $K$  over  $\mathbb{F}$  is an automorphism of  $K$  that fixes  $\mathbb{F}$ .

$$\text{Aut}(K/\mathbb{F}) = \{ \phi \in \text{Aut}(K) \mid \phi(x) = x \text{ for all } x \text{ in } \mathbb{F} \}$$

$$\text{Aut}(K) = \{ \phi \in \text{Aut}(K) \mid \phi(x) = x \text{ for all } x \text{ in } K \}$$

Since  $\mathbb{F}$  is subfield of  $K$

Every field is group

$\Rightarrow \text{Aut}(K/\mathbb{F})$  is subgroup for  $\text{Aut}(K)$

Theorem: let  $K/F$  be a field extension,

and  $\sigma \in \text{Aut}(K/F)$ . Then any polynomial  $f(x) \in F[x]$  which has  $\alpha \in K$  as a root, also has  $\sigma(\alpha) \in K$  as a root.

i.e.  $f(\alpha) = 0 \Leftrightarrow f(\sigma(\alpha)) = 0$ .

Equivalently, any polynomial with coefficient in  $F$  having  $\alpha$  as a root also has  $\sigma\alpha$  as a root.

i.e.  $\text{Aut}(K/F)$  permutes the roots of irreducible polynomials.

Proof: let  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$

$$a_i \in F$$

Suppose  $\alpha$  be a root of the polynomial

$$f(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n$$

where  $a_0, a_1, \dots, a_{n-1}$  are elements of

$F$ .

We know that  $\sigma$  is an additive

homomorphism.

Now applying the automorphism  $\sigma$ , we obtain

$$\begin{aligned} \sigma(a_0 + a_1\alpha + \dots + a_n\alpha^n) &= \sigma(0) \\ \sigma(a_0) + \sigma(a_1\alpha) + \dots + \sigma(a_{n-1}\alpha^{n-1}) &+ \sigma(a_n\alpha^n) = \sigma(0) = 0 \end{aligned}$$

Since  $\sigma$  is both additive and multiplicative

homomorphism

$$\begin{aligned} \sigma(a_0) + \sigma(\alpha)\sigma(a_1) + \dots + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} \\ + (\sigma(\alpha))^n \end{aligned}$$

$$= (\sigma(\alpha))^n + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} + \dots + \sigma(a_1)(\sigma(\alpha)) + \sigma(a_0) = 0$$

By assumption,  $\sigma \in \text{Aut}(K/F)$ , so

we have  $\sigma(a_i) = a_i$  for all  $i = 1, \dots, n$ .

Hence,

$$(\sigma\alpha)^n + a_{n-1}(\sigma\alpha)^{n-1} + \dots + a_1(\sigma\alpha) + a_0 = 0$$

This implies that  $\sigma\alpha$  is a root of the same polynomial over  $F$  as  $\alpha$ .

Therefore, any polynomial with coefficients in  $F$  having  $\alpha$  as a root also has  $\sigma\alpha$  as a root.

# Aut(K/F)

Let  $K = \mathbb{Q}(\sqrt{2})$ ,  $F = \mathbb{Q}$

$$\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \text{Aut}(K/F)$$

$\Rightarrow$  An automorphism  $\sigma$  of  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  is completely determined by the value of

$\sigma(\sqrt{2})$

The minimal polynomial of  $\sqrt{2}$  over  $\mathbb{Q}$  is  $x^2 - 2$ .

$$\Rightarrow (\sqrt{2})^2 - 2 = 0$$

Now applying  $\sigma$  to both sides, we have

$$\sigma(0) = \sigma((\sqrt{2})^2 - 2)$$

$$0 = \sigma(\sqrt{2})^2 - \sigma(2)$$

Since  $\sigma(2) = 2$

$$\Rightarrow \sigma(\sqrt{2})^2 = 2$$

Thus there are only two possibilities for  $\sigma(\sqrt{2})$ , namely

$$\boxed{\sigma(\sqrt{2}) = \sqrt{2}}$$

$$\text{and } \boxed{\sigma(\sqrt{2}) = -\sqrt{2}}$$

Therefore  $\mathbb{Q}$

$$\text{Aut}(\mathbb{Q}(\sqrt{2})) = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$$

$$= \{1, \sigma\}$$

Here 1 denote identity function

$$\text{i.e. } \sigma(\sqrt{2}) = \sqrt{2} \Rightarrow \sigma(x) = x$$

$\sigma$  denote conjugate of  $\sqrt{2}$  sending  $\sqrt{2} \rightarrow -\sqrt{2}$

$$\text{i.e. } \sigma(\sqrt{2}) = -\sqrt{2}$$

we can called  $\sigma(x) = -x$  conjugation automorphism

$$|\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2 \cong \mathbb{Z}_2$$

Similarly we can

## Fixed field of $G$

Let  $K/F$  be a field extension. For any subgroup  $G \subset \text{Aut}(K/F)$ , the collection of elements of  $K$  fixed by  $G$  is called a fixed field of  $G$ .

# Let  $K/F$  be a finite extension. Then  $K$  is said to be Galois over  $F$  and  $K/F$  is a Galois extension if the number of automorphisms equal to the degree of the extension.

$$|\text{Aut}(K/F)| = [K:F]$$

Let  $K/F$  be a finite extension such that  $|\text{Aut}(K/F)| = [K:F]$ . Then  $K$  is said to be Galois extension of  $F$ , the group  $\text{Aut}(K/F)$  is called the Galois group.

Galois group is denoted by

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

Note:

A field extension

$$E/F \text{ is}$$

called Galois if it is algebraic, separable and normal extension.

Note  $K/F$

put  $K = \mathbb{Q}(\sqrt{2})$ ,  $F = \mathbb{Q}$

Here  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ,  $\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = 2$

So the extension  $K/F$  is Galois with

Galois group

$$\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\} \cong \mathbb{Z}_2$$

where  $\sigma$  is the automorphism

$K/F$  is a Galois extension.

# The extension  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is not Galois because

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is not a normal extension.

$f(x) = x^3 - 2$  has 3 roots in  $\mathbb{C}$

$$\lambda_1 = \sqrt[3]{2} \in \mathbb{R}$$

$$\lambda_2 = \sqrt[3]{2} \left( \frac{-1 + i\sqrt{3}}{2} \right) \notin \mathbb{R}$$

$$\lambda_3 = \sqrt[3]{2} \left( \frac{-1 - i\sqrt{3}}{2} \right) \notin \mathbb{R}$$

$$(x - \lambda_1 \lambda_2) (x - \lambda_1 \lambda_3)$$

$$= (x^2 + \sqrt[3]{2}x + \sqrt[4]{4})$$

The field  $\mathbb{C}(\sqrt[3]{2})$  is contained in  $\mathbb{R}$ ,

but the other two roots of the irreducible

polynomial  $x^3 - 2$  are complex.

So the field extension contains only one

~~roots~~ root. This implies extension

is not normal.

Similarly we can say that

$$\text{Aut}(\mathbb{C}(\sqrt[3]{2})/\mathbb{C}) = 1.$$

$$\text{and } [\mathbb{C}(\sqrt[3]{2}) : \mathbb{C}] = 3$$

$$\text{But } \text{Aut}(\mathbb{C}(\sqrt[3]{2})/\mathbb{C}) \neq [\mathbb{C}(\sqrt[3]{2}) : \mathbb{C}]$$

# let  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  and  $F = \mathbb{Q}$ , then  
 the extension  $K/F$  is Galois  
 since  $K$  is the splitting field for the  
 polynomial  $(x^2-2)(x^2-3)$ .

Any automorphism  $\sigma \in \text{Aut}(K/F)$  is  
 completely determined by the image  
 $\sigma(\sqrt{2})$  and  $\sigma(\sqrt{3})$

Here  $\sqrt{2}$  and  $\sqrt{3}$  are roots of irreducible  
 polynomials  $x^2-2$  and  $x^2-3$  respectively.

Therefore we must have  $\sigma(\sqrt{2}) = \pm\sqrt{2}$   
 and  $\sigma(\sqrt{3}) = \pm\sqrt{3}$ .

So the only possibilities for automorphisms are  
 the map

$$\textcircled{1} \left\{ \begin{array}{l} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{array} \right.$$

$$\textcircled{2} \left\{ \begin{array}{l} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{array} \right.$$

$$(3) \begin{cases} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{cases}$$

$$(4) \begin{cases} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{cases}$$

We know that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$$

Since  $\sqrt{2} + \sqrt{3}$  satisfy the polynomial  $x^4 - 10x^2 + 1$  of degree 4 over  $\mathbb{Q}$ .

So the Galois group is of order 4.

Define the automorphisms  $\sigma$  and  $\tau$  by

$$\sigma : \begin{cases} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{cases}$$

$$\tau : \begin{cases} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{cases}$$

or more explicitly by

$$\sigma: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$\longrightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\tau: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$\longrightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3})$$
$$= (-\sqrt{2})(\sqrt{3})$$

$$\sigma(\sqrt{6}) = -\sqrt{6}$$

Then  $\sigma^2(\sqrt{2}) = \sigma(\sigma(\sqrt{2})) = \sigma(-\sqrt{2})$   
 $= \sqrt{2}$

$$\sigma^2(\sqrt{2}) = \sqrt{2}$$

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

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

$$\sigma^2 = \text{Id} = I$$

i.e.  $\sigma^2$  is identity automorphism

Similarly,  $\tau^2(\sqrt{2}) = \sqrt{2}$

$$\tau^2(\sqrt{3}) = \sqrt{3}$$

$$\tau^2 = \text{Id} = I$$

$\tau \in \sigma^2 \Rightarrow \tau^2 = I$  is the identity automorphism

The automorphism  $\sigma\tau$  can be computed.

$$\begin{aligned}\sigma\tau(\sqrt{2}) &= \sigma(\tau(\sqrt{2})) \\ &= \sigma(\sqrt{2})\end{aligned}$$

$$\sigma\tau(\sqrt{2}) = -\sqrt{2}$$

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

$\sigma\tau$  is conjugate automorphism

So  $\sigma\tau$  is the remaining non-trivial automorphism in the Galois group.

$$\text{Gal}(K/\mathbb{F})$$

Also,  $(\sigma\tau)^2 = (\sigma\tau)(\sigma\tau)(\sqrt{2})$

$$= (\sigma\tau)(-\sqrt{2})$$

$$= \sigma(\tau(-\sqrt{2}))$$

$$= \sigma(-\sqrt{2})$$

$$(\sigma\tau)^2(\sqrt{2}) = \sqrt{2}$$

$(\sigma\tau)^2 = \text{Id} = I$  is the identity.  
~~homom~~ automorphism.

clearly,  $\sigma$  and  $\tau$  generate  $\text{Gal}(K/F)$ .  
 and  $\text{Gal}(K/F)$  is isomorphic to the  
 Klein 4-group because  $\tau^2 = \sigma^2 = 1$ .

and  $(\sigma\tau)^2 = 1$

Therefore

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$$

$$= \{1, \sigma, \tau, \sigma\tau\}$$

$$\Rightarrow \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

we also have a bijection between the  
 subgroups  $G \subset \text{Gal}(K/F)$  and  
 extensions  $F \subset K^G \subset K$ , where  $K^G$   
 is the fixed field of  $G$ .

$$K^{\{1\}} = K$$

$$K^{\{1, \sigma\}} = \mathbb{Q}(\sqrt{3})$$

$$K^{\{1, \tau\}} = \mathbb{Q}(\sqrt{2})$$

$$K^{\{1, \sigma\tau\}} = \mathbb{Q}(\sqrt{6})$$

$$K^{\{\text{Gal}(K/F)\}} = \mathbb{Q}$$

$$K^{\{1, \sigma, \tau, \sigma\tau\}} = \mathbb{Q}$$

$$\text{since } \sigma(\sqrt{3}) = \sqrt{3}$$

$$\text{since } \tau(\sqrt{2}) = \sqrt{2}$$

$$\sigma\tau(\sqrt{2}\sqrt{3}) = \sqrt{3}\sqrt{2}$$

$$\sigma(\tau(\sqrt{6})) = \sqrt{6}$$

$$\sigma(\sqrt{6}) = \sqrt{6}$$

we can also determine the fixed  
 fields of the subgroup  $G$  of the  
 Galois Group by the following tables

<u>Subgroup. (<math>G</math>)</u>	<u>Fixed field. (<math>K^G</math>)</u>
$d \pm \gamma$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$d \pm, \sigma \gamma$	$\mathbb{Q}(\sqrt{3})$
$d \pm, \sigma \tau \gamma$	$\mathbb{Q}(\sqrt{6})$
$d \pm, \sigma, \tau, \sigma \tau \gamma$	$\mathbb{Q}$
$d \pm, \tau \gamma$	$\mathbb{Q}(\sqrt{2})$

Galois Group of the splitting field of  $p(x) = x^3 - 2$  over  $\mathbb{Q}$ .

=> Splitting of  $x^3 - 2$  over  $\mathbb{Q}$  is  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

where  $\zeta_3 = \frac{-1 + \sqrt{-3}}{2}$

The roots of  $x^3 - 2$  over  $\mathbb{Q}$  are  $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$  where  $\rho = \zeta_3 = \frac{-1 + \sqrt{-3}}{2}$

and  $\zeta_3$  is a primitive cube root of unity.

i.e.  $x^3 - 2 = (x - \sqrt[3]{2})(x - \rho\sqrt[3]{2})(x - \rho^2\sqrt[3]{2})$

$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$  can be written as  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$  or  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$

Here  $1, \sqrt[3]{2}, \sqrt[3]{2}^2$  form a basis for  $\mathbb{Q}(\sqrt[3]{2})$  over  $\mathbb{Q}$

$1, i\sqrt{3}$  form a basis for  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$  over  $\mathbb{Q}(\sqrt[3]{2})$

$$[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}]$$

$$= [\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

$$= 2 \cdot 3$$

$$= 6$$

$$[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$$

$$1, \sqrt[3]{2}, \sqrt[3]{2}^2, (i\sqrt{3}), (\sqrt[3]{2} \cdot i\sqrt{3}), (\sqrt[3]{2}^2 \cdot i\sqrt{3})$$

form a basis for  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$  over  $\mathbb{Q}$ ,

we can also write  $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}]$  basis

is

$$\{ a + bi\sqrt{3} + c\sqrt[3]{2} + d(\sqrt[3]{2})^2 + e\sqrt[3]{2}\sqrt{3}i + f(\sqrt[3]{2})^2i\sqrt{3} : a, b, c, d, e, f \in \mathbb{Q} \}$$

Since the minimal polynomial of  $\sqrt[3]{2}$

over  $\mathbb{Q}$  is  $x^3 - 2$ .

Any automorphism of  $K/\mathbb{Q}$  must

send  $\sqrt[3]{2}$  to one of the three roots  $\sqrt[3]{2}$ ,  $\sqrt[3]{2}\zeta_3$  and  $\sqrt[3]{2}\zeta_3^2$

Here  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

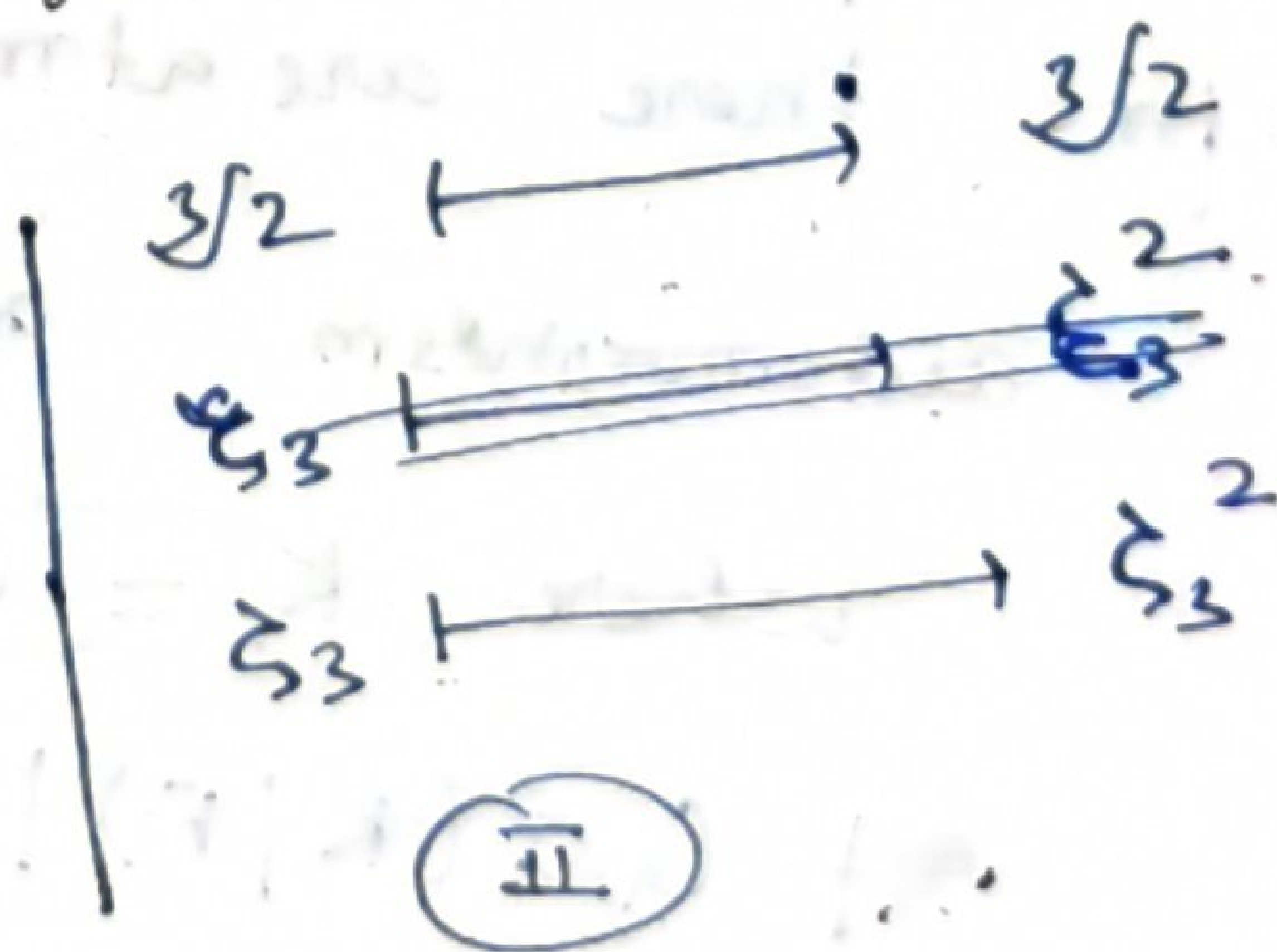
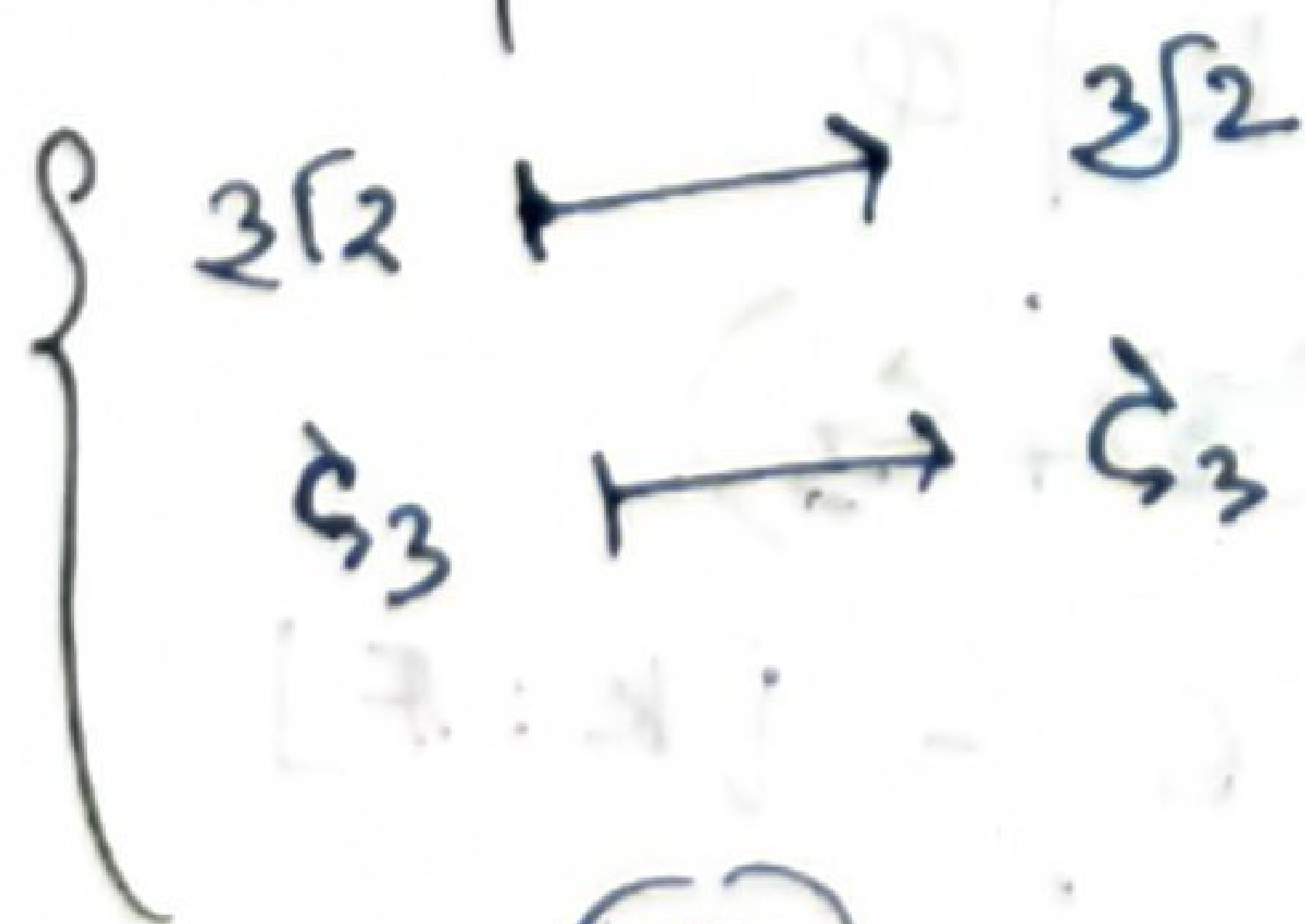
Similarly, the minimal polynomial of  $\zeta_3$  over

$\mathbb{Q}$  is  $x^2 + x + 1$ .

Any automorphism of  $K/\mathbb{Q}$  must send

$\zeta_3$  to one of the two roots  $\zeta_3, \zeta_3^2$ .

Now only possible maps for automorphisms are the



$\zeta_3 = e^{2\pi i/3}$   
 $\zeta_3^2 = e^{4\pi i/3}$

$$(iii) \left\{ \begin{array}{l} \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \\ \mathbb{Q}(\zeta_3) \longrightarrow \mathbb{Q}(\zeta_3) \end{array} \right.$$

$$(iv) \left\{ \begin{array}{l} \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \\ \mathbb{Q}(\zeta_3) \longrightarrow \mathbb{Q}(\zeta_3^2) \end{array} \right.$$

$$(v) \left\{ \begin{array}{l} \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, \zeta_3^2) \\ \mathbb{Q}(\zeta_3) \longrightarrow \mathbb{Q}(\zeta_3) \end{array} \right.$$

$$(vi) \left\{ \begin{array}{l} \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, \zeta_3^2) \\ \mathbb{Q}(\zeta_3) \longrightarrow \mathbb{Q}(\zeta_3^2) \end{array} \right.$$

Therefore there are at most 6 possible

automorphisms of  $K|\mathbb{Q}$

where  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

$$|\text{Gal}(K|\mathbb{Q})| = 6 = [K:\mathbb{Q}]$$

where  $\mathbb{F} = \mathbb{Q}$

Define the automorphism  $\sigma$  and  $\tau$  by

$$\sigma : \begin{cases} \sqrt[3]{2} \longrightarrow \rho \sqrt[3]{2} \\ \zeta_3 \longmapsto \zeta_3 \end{cases} \quad \text{Here } \rho = \zeta_3$$

$$\tau : \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \\ \zeta_3 \longrightarrow \zeta_3^2 = -1 - \zeta_3 \end{cases}$$

Here  $\zeta_3 = \frac{-1 + \sqrt{-3}}{2}$

$$\zeta_3^2 = -1 + \frac{1}{2} - \frac{\sqrt{-3}}{2}$$

$$= -\frac{1}{2} - \frac{\sqrt{-3}}{2}$$

$$\zeta_3^2 = \frac{-1 - \sqrt{-3}}{2}$$

$$\boxed{\zeta_3^2 = -1 - \zeta_3}$$

We know that the basis of  $\mathbb{Q}(\sqrt[3]{2}, \rho)$  are  $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho\sqrt[3]{2}, \rho(\sqrt[3]{2})^2\}$ .

Here  $\rho = \zeta_3$

Also, we can write  $\rho = i\sqrt{3}$   
 since  $i\sqrt{3} = \sqrt{-3}$

Here, one automorphism  $\sigma$  with  $\sigma(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}\zeta_3, \zeta_3)$  is the map

By choosing a basis for  $K/\mathbb{Q} = (\mathbb{Q}(\sqrt[3]{2}, \rho)/\mathbb{Q})$

We can describe the  $\sigma$  map completely

$$\text{explicitly as } \sigma(c_1 + c_2\sqrt[3]{2} + c_3\sqrt[3]{4} + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3 + c_6\sqrt[3]{4}\zeta_3)$$

$$= c_1 + c_2\sqrt[3]{2}\zeta_3 + c_3\sqrt[3]{4}\zeta_3^2 + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3^2 + c_6\sqrt[3]{4}$$

Another automorphism is the map  $\tau$  with  $\tau(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3^2)$

$$\tau(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3^2)$$

$$\Rightarrow \tau \tau(\sqrt[3]{2}, \zeta_3) = \tau^2(\sqrt[3]{2}, \zeta_3)$$

$$\Rightarrow \tau(\sqrt[3]{2}, \zeta_3^2) = (\sqrt[3]{2}, \zeta_3^4)$$

(we know) that  $\zeta_3 = e^{2\pi i/3}$

$$\zeta_3^3 = (e^{2\pi i/3})^3 = e^{2\pi i}$$

$$\zeta_3^3 = 1$$

$$\zeta_3^4 = \zeta_3^3 \cdot \zeta_3 = 1 \cdot \zeta_3$$

$$\text{So } \tau^2(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3)$$

$$\text{i.e. } \tau^2 = \text{Id (identity automorphism)}$$

$$\text{i.e. Id denotes } \boxed{\mathbb{I}(x) = x}$$

$$\text{where } x = (\sqrt[3]{2}, \zeta_3)$$

$$\mathbb{I} = \tau$$

Similarly,  $\sigma(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2} \zeta_3, \zeta_3)$

$$\Rightarrow \sigma^2(\sqrt[3]{2}, \zeta_3) = \sigma(\sigma(\sqrt[3]{2}, \zeta_3))$$

$$= \sigma(\sqrt[3]{2} \zeta_3, \zeta_3)$$

$$= (\sqrt[3]{2} \zeta_3^2, \zeta_3)$$

$$\sigma^3(\sqrt[3]{2}, \zeta_3) = \sigma(\sigma^2(\sqrt[3]{2}, \zeta_3))$$

$$= \sigma(\sqrt[3]{2} \zeta_3^2, \zeta_3)$$

$$= \sigma(\sqrt[3]{2} \zeta_3^3, \zeta_3)$$

$$\sigma^3(\sqrt[3]{2}, \zeta_3) = \sigma(\sqrt[3]{2}, \zeta_3)$$

$$\Rightarrow \sigma^3 = \text{Id} \quad (\text{identity has automorphism})$$

Now  $\sigma\tau$  is the map

$$\sigma(\tau(\sqrt[3]{2}, \zeta_3))$$

$$= \sigma(\sqrt[3]{2}, \zeta_3^2)$$

$$= \sigma(\sqrt[3]{2} \zeta_3^2)$$

$$= (\sqrt[3]{2} \zeta_3, \zeta_3^2)$$

$$\tau(\sigma(\sqrt[3]{2}, \zeta_3))$$

$$\tau = \sqrt[3]{2}$$

$$\Rightarrow \tau(\sqrt[3]{2} \zeta_3, \zeta_3) = (\sqrt[3]{2} \zeta_3^2, \zeta_3^2)$$

$$\tau : \begin{cases} \zeta_3 \longrightarrow \zeta_3^2 \\ \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \end{cases}$$

$$\tau(\sqrt[3]{2} \zeta_3, \zeta_3) = (\sqrt[3]{2} \zeta_3^2, \zeta_3^2)$$

Also, we can write

$$\tau(\sqrt[3]{2} \zeta_3) = \tau(\sqrt[3]{2}) \tau(\zeta_3)$$

Since  $\tau$  is an automorphism  
so  $\tau$  is homomorphism

we know

$$\tau : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}$$

$$\text{so } \tau(\sqrt[3]{2}) = \sqrt[3]{2}$$

$$\text{Similarly } \tau(\zeta_3) = \zeta_3^2$$

$$\text{Therefore } \left\{ \begin{aligned} \tau(\sqrt[3]{2}\zeta_3) &= \tau(\sqrt[3]{2})\tau(\zeta_3) \\ &= \sqrt[3]{2}\zeta_3^2 \end{aligned} \right.$$

This implies that  $\sigma\tau \neq \tau\sigma$

$$\text{and } \sigma^3 = \tau^2 = 1.$$

$$\text{Hence: } \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \langle \sigma, \tau \rangle$$

$$\text{ie } \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong S_3$$

Q. Prove that  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{3})$  are not isomorphic.

Soln:

Suppose there is an isomorphism

$$f: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3}) \text{ then}$$

$$f(\sqrt{2}) = a + b\sqrt{3}$$

we know that every field is ring

in ring homomorphism, multiplicative identity preserved i.e.  $f: A \rightarrow B$

$$f(1_A) = f(1_B) = 1_B$$

Therefore  $2 = (\sqrt{2})^2$

$$2 = 2 \cdot f(1)$$

since  $f(1) = 1$

$$= f(2 \cdot 1)$$

$$\boxed{2 = f(2)}$$

But  $f(2) = f((\sqrt{2})^2) = f(\sqrt{2}) \cdot f(\sqrt{2})$

$$= f(\sqrt{2}) \cdot f(\sqrt{2})$$

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

$$= (a + b\sqrt{3})^2$$

$$f(2) = a^2 + 3b^2 + 2ab\sqrt{3}$$

$$2 = a^2 + 3b^2 + 2ab\sqrt{3}$$

We know  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ ,

$$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}.$$

We know that  $1$  and  $\sqrt{3}$  are linearly

independent over  $\mathbb{Q}$

Proof: If  $a \cdot 1 + b \cdot \sqrt{3} = 0$  for some  $a, b \in \mathbb{Q}$

then we have to show that

$$a = b = 0$$

if  $b = 0$  i.e.  $b$  must be  $0$

because if  $b \neq 0$ , then  $a = -b\sqrt{3}$

$$\Rightarrow \sqrt{3} = \frac{a}{-b}$$

$$\text{i.e. } -a/b \in \mathbb{Q}$$

Contradiction that  $\frac{a}{b} \in \mathbb{Q}$

Therefore  $a = 0$

Also,  $b = 0$ .

Thus 1 and  $\sqrt{3}$  are linearly independent over  $\mathbb{Q}$ .

Note:- Two non-zero real numbers  $r_1$  and  $r_2$  are linearly independent over  $\mathbb{Q}$  if

$$\frac{r_1}{r_2} \notin \mathbb{Q} \text{ irrational.}$$

Since 1 and  $\sqrt{3}$  are linearly independent over  $\mathbb{Q}$  so  $2ab = 0$   
i.e. either  $a = 0$  or  $b = 0$

$$\text{If } a = 0, \text{ then } 3b^2 = 2$$

$$\Rightarrow b = \sqrt{\frac{2}{3}} \notin \mathbb{Q}$$

$$\text{If } b = 0 \Rightarrow a = \sqrt{2} \notin \mathbb{Q}$$

So in both cases we are getting contradiction

Therefore  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{3})$  are not isomorphic.

Q. Determine the automorphisms of the extension  $\mathbb{Q}(\sqrt[4]{2}) / \mathbb{Q}(\sqrt{2})$  explicitly.

Soln: The minimal polynomial for  $\sqrt[4]{2}$  over  $\mathbb{Q}(\sqrt{2})$  is  $x^2 - \sqrt{2}$

Roots of  $f(x) = x^2 - \sqrt{2}$  are

$$+ \sqrt[4]{2}, - \sqrt[4]{2}$$

$$\Rightarrow x^2 = \sqrt{2}$$

$$\Rightarrow x = (\sqrt{2})^{1/2}$$

$$= \pm \sqrt[4]{2}$$

Hence the only possible possibilities for automorphisms are the map

$$\left\{ \begin{array}{l} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ \sqrt[4]{2} \mapsto -\sqrt[4]{2} \end{array} \right.$$

$$\left\{ \begin{array}{l} -\sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ -\sqrt[4]{2} \mapsto \sqrt[4]{2} \end{array} \right.$$

i.e. we can write and classify the map in given following way

$$\left\{ \begin{array}{l} 4\sqrt{2} \longmapsto 4\sqrt{2} \\ -4\sqrt{2} \longmapsto -4\sqrt{2} \end{array} \right. \Rightarrow \text{identity} = 1 \text{ function.}$$

$$\left\{ \begin{array}{l} 4\sqrt{2} \longmapsto -4\sqrt{2} \\ -4\sqrt{2} \longmapsto 4\sqrt{2} \end{array} \right. \Rightarrow \sigma.$$

$\sigma$  denote the automorphism that map elements to their conjugates.

Aut  $(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  consists of two elements  $1 = \text{id}$  and  $\sigma$ , where  $\sigma$  satisfy

$$\sigma(4\sqrt{2}) = -4\sqrt{2} \quad \text{or} \quad \sigma(-4\sqrt{2}) = 4\sqrt{2}$$

$$1 = \text{id}(4\sqrt{2}) = 4\sqrt{2} \quad \text{or} \quad \text{id}(-4\sqrt{2}) = -4\sqrt{2}$$

Hence  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \langle 1, \sigma \rangle \cong \mathbb{Z}_2$

~~Q~~ Prove that any continuous map on  $\mathbb{R}$  which is the identity on  $\mathbb{Q}$  is the identity map, hence  $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$ .

Soln: Since  $\mathbb{Q}$  is dense in  $\mathbb{R}$ , for any  $q \in \mathbb{R}$  there exist a sequence  $\{q_n\} \subset \mathbb{Q}$  that converge to  $q$ .

$$\text{i.e. } q = \lim_{n \rightarrow \infty} q_n$$

$$= \lim_{n \rightarrow \infty} \sigma(q_n)$$

Since  $\sigma$  is a homeomorphism as well as an automorphism

$$= \sigma\left(\lim_{n \rightarrow \infty} q_n\right)$$

$$= \sigma(q)$$

$$\boxed{q = \sigma(q)}$$

$$\boxed{\sigma(q) = q}$$

We know that  $\mathbb{Q}$  is dense in  $\mathbb{R}$ .  
proof: Take  $a, b \in \mathbb{Q}$  such that  $a < b$ .

$$\text{Set } r = \frac{a+b}{2}$$

Then  $U = \{x \in \mathbb{Q} : x < r\}$

$V = \{x \in \mathbb{Q} : x > r\}$

$$U \cap V = \emptyset$$

$U$  and  $V$  are open disjoint-sets containing  $a$  and  $b$ .

Therefore  $\mathbb{Q}$  is Hausdorff.

So  $q_n \rightarrow \gamma$  because in Hausdorff space every convergent sequence is unique.

$$q_n \rightarrow \gamma$$

$$\Rightarrow \sigma \gamma = \gamma$$

$\Rightarrow \sigma$  is the identity on  $\mathbb{R}$ .

Thus every automorphism which preserves  $\mathbb{Q}$  must be the identity.

$$\text{So } \text{Aut}(\mathbb{R}/\mathbb{Q}) = 1.$$

Q. Determine the splitting field in  $\mathbb{C}$  for  
 $x^p - 1$  over  $\mathbb{Q}$ .

Soln. let  $\mathbb{F}$  be a splitting field for  
 $f_p(x) = x^p - 1$  and let  $\zeta_p = e^{2\pi i/p}$

Here actually, the roots of  $f_p(x)$  are

$$\left\{ \zeta_p^j : 0 \leq j \leq p-1 \right\}$$

It follows that  $\mathbb{F} = \mathbb{Q}(\zeta_p)$

# Fundamental theorem of Galois theory.

(1)  $K = \mathbb{Q}(2^{1/3}, \zeta_3) / \mathbb{Q}$  with the

automorphisms

$$\sigma(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3)$$

$$\tau(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$$

The fixed fields of the subgroup  $\{e\}, \langle \tau \rangle,$   
 $\langle \sigma \rangle$  and  $\langle \tau, \sigma \rangle$

are respectively  $\mathbb{Q}(2^{1/3}, \zeta_3), \mathbb{Q}(2^{1/3}),$

$\mathbb{Q}(2^{1/3}\zeta_3), \mathbb{Q}(2^{1/3}\zeta_3^2), \mathbb{Q}(\zeta_3)$  and  $\mathbb{Q}$

These

0. Determine the Galois group of  
 $(x^2-2)(x^2-3)(x^2-5)$ . Determine ~~the~~  
 all the ~~sub~~ subfields of the splitting  
 field of these polynomials.

soln.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  is the splitting  
 field of the polynomial  $f(x) = (x^2-2)(x^2-3)(x^2-5)$   
 over  $\mathbb{Q}$ .

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$  is a

$\mathbb{Q}$ -basis for  $K$

and thus  $[K:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}]$

$$= [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$$

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

$$= 8$$

so if  $G = \text{Gal}(K/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$

then  $|G| = 8$

Consider the following automorphisms in  $G$ :

$$\sigma_2: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$$

$$\sigma_3: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$$

$$\sigma_5: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

It is obvious that ~~for~~ for any such automorphism  $\sigma$  we have that

$$(\sigma^2)(\sqrt{K}) = \sqrt{K} \text{ for any } K = 2, 3, 5.$$

$$\text{e.g. } \sigma_2^2(\sqrt{2}) = \sqrt{2} \Rightarrow \sigma_2(\sigma(\sqrt{2})) = \sqrt{2}$$

$$\sigma_2^2(\sqrt{3}) = \sqrt{3}$$

$$\sigma_2^2(\sqrt{5}) = \sqrt{5}$$

This implies  $\sigma_2^2 = I_2$  where  $I_2$  is  
Identity function.

$$\text{order } g(\sigma_2) = 2.$$

Similarly  $\text{order } g(\sigma_3)$  and  $|\sigma_5| = 2.$

Thus all the automorphisms are of order 2  
and we conclude that the Galois group is

$$G = \langle \sigma_2, \sigma_3, \sigma_5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\langle \sigma_2 \rangle \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2$$

$$\langle \sigma_3 \rangle \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2.$$

$$\langle \sigma_5 \rangle \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2$$

This implies  $G = \text{Gal}(K/\mathbb{Q})$  is  
abelian.

Since  $G$  is abelian, so all of its subgroups are normal.

Now by the Fundamental theorem of Galois theory, every normal subgroup  $H \leq G$

corresponds to a subfield  $K^H$ , which is a splitting field over  $\mathbb{Q}$ .

Since  $|H|$  divides 8, we distinguish 4 cases.

(1) If  $|H| = 1$ , then clearly  $K^H = K$ .

where  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

(2) If  $|H| = 2$ , then  $H$  contains the identity and an element of order 2, so it can be any of the following 7 groups.

(1)  $\{1, \sigma_2\}$

(2)  $\{1, \sigma_3\}$

(3)  $\{1, \sigma_5\}$

(4)  $\{1, \sigma_2\sigma_3\}$

(5)  $\{1, \sigma_5\sigma_2\}$

(6)  $\{1, \sigma_2\sigma_3\sigma_5\}$

Now by using Galois correspondence properties

$$H \longmapsto K^H = \{ x \in K : \sigma(x) = x \text{ for all } \sigma \in H \}$$

The corresponding fixed subfields of the given group are :-

$$(1) H_1 = \langle \sigma_2 \rangle$$

$$\sigma_2 \begin{cases} \sqrt{2} & \longrightarrow -\sqrt{2} \\ \sqrt{3} & \longrightarrow \sqrt{3} \\ \sqrt{5} & \longrightarrow \sqrt{5} \end{cases}$$

Here  $\sigma(\sqrt{2}) = -\sqrt{2}$  not satisfying the property  $\sigma(x) = x$ . ✓

Therefore  $K^H \Rightarrow K^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ .

Therefore the fixed field of the subgroup

$$H_1 = \langle \sigma_2 \rangle \text{ is } \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

Similarly the remaining corresponding fixed subfields are  $\mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{5}, \sqrt{6}), \mathbb{Q}(\sqrt{2}, \sqrt{15}), \mathbb{Q}(\sqrt{3}, \sqrt{10}), \mathbb{Q}(\sqrt{6}, \sqrt{10})$

③ If  $|H| = 4$ , then  $H$  contains the identity, two distinct elements of order 2 and their product so it can be any of the following 7 groups:

$$\{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\}, \{1, \sigma_3, \sigma_5, \sigma_3\sigma_5\}$$

$$\{1, \sigma_5, \sigma_2, \sigma_5\sigma_2\}, \{1, \sigma_2, \sigma_3\sigma_5, \sigma_2\sigma_3\sigma_5\},$$

$$\{1, \sigma_3, \sigma_2\sigma_5, \sigma_2\sigma_3\sigma_5\}, \{1, \sigma_5, \sigma_2\sigma_3, \sigma_2\sigma_3\sigma_5\},$$

$$\{1, \sigma_2\sigma_3, \sigma_3\sigma_5, \sigma_5\sigma_2\}.$$

Their corresponding fixed subfields are

$$\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{15}), \mathbb{Q}(\sqrt{10}),$$

$$\mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{30})$$

④ If  $|H| = 8$ , then  $K^H = \mathbb{Q}$ .

Q.

Let  $p$  be a prime. Determine the elements of the Galois group of  $x^{p-2}$ .

Soln

The roots of the polynomial  $x^{p-2}$  are

$$\sqrt[p]{2} \zeta^K, \text{ where } K = 0, 1, \dots, p-1,$$

and  $\sqrt[p]{2}$  is a real  $p$ th root of 2 and  $\zeta$  is a primitive root of unity.

$$\zeta = e^{2\pi i/p}$$

Thus  $x^{p-2}$  is a ~~sepa~~ separable polynomial over  $\mathbb{Q}$ . The Galois group of  $x^{p-2}$  is the Galois group of the splitting field of  $x^{p-2}$ .

The splitting field of  $x^{p-2}$  is

$$K = \mathbb{Q}(\sqrt[p]{2}, \zeta)$$

degree  $p(p-1)$

Since  $\sqrt[p]{2}$  is a root of  $x^p - 2$ , the

degree of extension  $[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}(\zeta)] \leq p$

Thus we have

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}(\zeta)] [\mathbb{Q}(\zeta) : \mathbb{Q}]$$
$$\leq p(p-1) = p(p-1)$$

Also, the degree of cyclotomic extension

over  $\mathbb{Q}$  is  $\phi(p) = p-1$  where

$\phi$  is the Euler  $\phi$  function.

Let  $G = \text{Gal}(K/\mathbb{Q})$  be the Galois group of  $x^p - 2$ . The order of the Galois group  $G$  is  $p(p-1)$ .

Let  $\sigma \in G$  be an automorphism.

Then  $\sigma$  sends an element of  $G$  to its conjugates.

Note: Conjugates are the roots of the minimal polynomial  $P_{K, \alpha}(x)$  of  $\alpha$  over  $K$ .

The minimal polynomial of  $\sqrt[p]{2}$  is  $x^p - 2$

The minimal polynomial of  $\zeta$  is the cyclotomic polynomial

$$\phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1.$$

Therefore,  $\sigma$  map

$$\sqrt[p]{2} \longrightarrow \sqrt[p]{2} \zeta^a$$

$$\zeta \longrightarrow \zeta^b$$

for some  $a = 0, 1, \dots, p-1$

and  $b = 1, 2, \dots, p-1$ .

Thus, there are  $p(p-1)$  possible maps for  $\sigma$ .

Since the order of  $G$  is  $p(p-1)$ , these are exactly the elements of the Galois group  $G$  of the polynomial  $x^p - 2$