Galois Theory

Automorphism of field K

An isomorphism from field K to itself is called Automorphism.

The collection of automorphism of K is denoted by $Aut(K)$.

If $\alpha \in K$ then we will write $\sigma\alpha$ for $\sigma(\alpha)$

An automorphism $\sigma in Aut(K)$ is said to fix an element $\alpha \in K$ if $\sigma\alpha = \alpha$.

If F is a subset of K the automorphism σ is said to fix F if it fixes all the elements of F that is $\sigma\alpha = \alpha \forall \alpha \in F$

Note: Any field has atleast one automorphism that is the identity map.

Notation: Let K/F be an extension of fields. Let $Aut(K/F)$ be the collection of automorphism of K which fixes F

Proposition: $Aut(K)$ is a group under composition and $Aut(K/F)$ is a subgroup.

Proof: Since $Aut(K)$ is the set of all automorphisms of field K.
Let σ and $\tau \in Aut(K)$ since composition of two isomorphism is an isomorphism so $\sigma\tau \in Aut(K)$ so $Aut(K)$ is closed with respect to composition.
Associativity holds and identity elements is identity map
Since map is onto so inverse exists for every nonzero map in $Aut(K)$
Hence $Aut(K)$ is a group under composition.
Now to show $Aut(K/F)$ is a subgroup of $Aut(K)$
Let σ and $\tau \in Aut(K/F)$ that is σ, τ fixes F so for $a \in F$
$\sigma\tau(a) = \sigma(\tau(a)) = \sigma(a) = a$ this is true for every $a \in F$ so $\sigma\tau \in Aut(K/F)$. Now for any $\sigma \in Aut(K/F)$ $\sigma(a) = a$ so $\sigma^{-1}(a) = a$ so $\sigma^{-1} \in Aut(K/F)$ hence $Aut(K/F)$ is a subgroup of $Aut(K)$.

Proposition: Let K/F be field extension and let $\alpha \in K$ be an algebraic over F. Then for any $\sigma \in Aut(K/F)\sigma\alpha$ is a root of the minimal polynomial for α over F that is $Aut(K/F)$ permutes the roots of irreducible polynomial. Equivalently, any polynomial with coefficient in F having α as a root also has $\sigma\alpha$ as a root.

Proof: Let K/F be a field extension and let α be an algebraic over F then α satisfies a polynomial $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0$, where $a_i \in F$

so we have $\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + ... + a_1\alpha + a_0 = 0$

Applying automorphism σ we get

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

Using the fact that σ is also a multiplicative homomorphism this becomes

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

By assumption, σ fixes all the elements of F, so $\sigma(a_i) = a_i, i = 0, 1, \ldots, n-1$. Hence

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

But this says precisely that $\sigma\alpha$ is a root of the same polynomial over F as α.

Examples

Let $K = \mathbb{Q}(\sqrt{2})$. If $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\tau(\sqrt{2}) = \pm\sqrt{2}$ since these are the two roots of the minimal polynomial for $\sqrt{2}$. Since τ fixes $\mathbb{Q}$, this determines τ completely:

$$\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}.$$

The map $\sqrt{2} \mapsto \sqrt{2}$ is just the identity automorphism 1 of $\mathbb{Q}(\sqrt{2})$. The map $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ is the isomorphism

Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$

Let $K = \mathbb{Q}(\sqrt[3]{2})$. As before, if $\tau \in \mathrm{Aut}(K/\mathbb{Q})$, then τ is completely determined by its action on $\sqrt[3]{2}$ since

$$\tau(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\tau\sqrt[3]{2} + c(\tau\sqrt[3]{2})^2.$$

Since $\tau\sqrt[3]{2}$ must be a root of $x^3 - 2$ and the other two roots of this equation are not elements of K

only possibility is $\tau\sqrt[3]{2} = \sqrt[3]{2}$ i.e., $\tau = 1$. Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$ is the trivial group.

Proposition Let $H \leq \mathrm{Aut}(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.

Proof: Let $h \in H$ and let $a, b \in F$. Then by definition $h(a) = a$, $h(b) = b$ so that $h(a \pm b) = h(a) \pm h(b) = a \pm b$, $h(ab) = h(a)h(b) = ab$ and $h(a^{-1}) = h(a)^{-1} = a^{-1}$, so that F is closed, hence a subfield of K.

Definition. If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all the elements of H is called the *fixed field* of H.

Proposition:

1) If $F_1 \subset F_2 \subset K$ are two subfields of K then $Aut(K/F_2) \leq Aut(K/F_1)$

2) If $H_1 \leq H_2 \leq Aut(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2 respectively then $F_2 \subset F_1$

Proof:

1) Suppose $F_1 \subset F_2$ we have to show that $Aut(K/F_2) \leq Aut(K/F_1)$

since both are groups so it is sufficient to show that $Aut(K/F_2) \subset Aut(K/F_1)$

Let $\sigma \in Aut(K/F_2)$ so σ is an isomorphism from K to itself and it fixes F_2 since $F_1 \subset F_2$ so σ also fixes F_1 therefor $\sigma \in Aut(K/F_1)$ hence $Aut(K/F_2) \leq Aut(K/F_1)$.

2) Suppose $H_1 \leq H_2$ since $H_1 =$ Set of all automorphism which fixes F_1 and $H_2 =$ Set of all automorphism which fixes F_2

To show $F_2 \subset F_1$

Let $a \in F_2$ and since $\sigma(a) = a$ for $\sigma \in H_2$ and as $H_1 \leq H_2$ then every element of H_1 is and element of H_2 that is $\delta \in H_1$ then $\delta \in H_2$ since *delta* fixes every element of F_1 also $delta(a) = a$ for $a \in F_2$ so a inF_1 hence $F_2 \subset F_1$.

Examples

(1) Suppose $K = \mathbb{Q}(\sqrt{2})$ as in Example 1 above. Then the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ will be the set of elements of $\mathbb{Q}(\sqrt{2})$ with

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

since everything is fixed by the identity automorphism. This is the equation

$$a - b\sqrt{2} = a + b\sqrt{2}.$$

which is equivalent to $b = 0$, so the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is just $\mathbb{Q}$.

(2) Suppose now that $K = \mathbb{Q}(\sqrt[3]{2})$ as in Example 2 above. In this case $\mathrm{Aut}(K) = 1$, so that every element of K is fixed, i.e., the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is $\mathbb{Q}(\sqrt[3]{2})$.

Proposition: Let E be a splitting field over F of the polynomial $f(x) \in F[x]$. Then $|Aut(E/F)| \leq [E : F]$ with equality if $f(x)$ is separable over F.

Proof: Let F be a field and E be the splitting field over F of $f(x) \in F[x]$.Since we know that if there is an isomorphism between F and F' then there exist an isomorphism between its splitting field that is E and E'. we will show by mathematical induction on $[E : F]$.
If $[E : F] = 1$ then $E = F$ so $E' = F'$ then $\sigma = \phi$ then number of extension is 1
If $[E : F] > 1$ then $f(x)$ has at least one irreducible factor say $p(x)$ of degree > 1 corresponding to this $p'(x)$ of $f'(x)$. Let α be a root of $p(x)$. If σ be any extension of ϕ to E then σ restricted to a subfield $F(\alpha)$ of E is an isomorphism τ of $F(\alpha)$ to some subfield $F'(\beta)$ of E'.
Since the isomorphism τ completely determined by the action on α that is by $tau(\alpha)$ since α generates $F(\alpha)$ over F so $\tau\alpha$ be a root say β of $p'(x)$.

$$\begin{array}{lccc} \sigma: & E & \xrightarrow{\sim} & E' \\ & | & & | \\ \tau: & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & | & & | \\ \varphi: & F & \xrightarrow{\sim} & F' \end{array}$$

Since to count the number of extensions we need to count number of this possible diagrams. The number of extensions ϕ to an isomorphism τ is equal to the number of distinct roots β of $p'(x)$. Since the degree of $p(x)$ and $p'(x)$ are both equal to $[F(\alpha) : F]$ so number of extensions of ϕ to τ is atmost $[F(\alpha) : F]$
So equality holds if $p(x)$ has distinct roots.
Since E is a splitting field for $f(x)$ over $F(\alpha)$ and E' is a splitting field of $f'(x)$ over $F'(\beta)$ and $[E : F(\alpha)] < [E : F]$.
by induction the number of extensions of *tau* to σ is $\leq [E : F(\alpha)]$.
Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ so the number of extensions of ϕ to σ is $\leq [E : F]$ and equality holds if $f(x)$ has distinct roots.
Hence $|Aut(E/F)| \leq [E : F]$

Definition. Let K/F be a finite extension. Then K is said to be *Galois* over F and K/F is a *Galois* extension if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois the group of automorphisms $\mathrm{Aut}(K/F)$ is called the *Galois group of* K/F, denoted $\mathrm{Gal}(K/F)$.

Corollary 6. If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

Proof:Since polynomial is separable so it has distinct roots so number of automorphisms is equal to degree of polynomial and since $[K : F] = deg f(x)$. Therefore $|Aut(K/F)| = [K : F]$.

Definition. If $f(x)$ is a separable polynomial over F, then the *Galois group of* $f(x)$ *over* F is the Galois group of the splitting field of $f(x)$ over F.

Examples

(1) The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois with Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ where σ is the automorphism

$$\sigma : \mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2})$$
$$a + b\sqrt{2} \longmapsto a - b\sqrt{2}.$$

(2) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since its group of automorphisms is only of order 1.

(3)

To find $Aut(Q(\sqrt{2},\sqrt{3})/Q)$
Since it is the splitting field for the polynomial $(x^2-2)(x^2-3)$
So any automorphism can be determined by the action on generators $\sqrt{2}$ and $\sqrt{3}$
Since $\sqrt{2}$ maps to $\pm\sqrt{2}$ and $\sqrt{3}$ maps to $\pm\sqrt{3}$.
So we have four choice that is

$$\begin{cases}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\end{cases}\quad\begin{cases}\sqrt{2}\mapsto-\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\end{cases}\quad\begin{cases}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto-\sqrt{3}\end{cases}\quad\begin{cases}\sqrt{2}\mapsto-\sqrt{2}\\ \sqrt{3}\mapsto-\sqrt{3}\end{cases}.$$

Define the automorphisms σ and τ by

$$\sigma:\begin{cases}\sqrt{2}\mapsto-\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\end{cases}\qquad\tau:\begin{cases}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto-\sqrt{3}\end{cases}$$

Since any element in $Q(\sqrt{2},\sqrt{3})$ can be written as $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$
So $\sigma : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$
And $\tau : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$
Since $\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = (\sigma(\sqrt{2}))(\sigma(\sqrt{3})) = -\sqrt{2}\sqrt{3} = -\sqrt{6}$
Similarly for τ

Since $\sigma^2(\sqrt{2}) = \sigma(\sigma\sqrt{2}) = \sigma(-\sqrt{2}) = \sqrt{2}$
and $\sigma^2(\sqrt{3}) = \sigma(\sigma\sqrt{3}) = \sigma(\sqrt{3}) = \sqrt{3}$
Hence $\sigma^2 = I$ Similarly $\tau^2 = I$

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

$Gal(Q(\sqrt{2}, \sqrt{3})/Q) = \{1, \sigma, \tau, \sigma\tau\}$

This Galois group is isomorphic to Klein 4-group. Now to find Subgroups of this Galois group.

Since Subgroups are $\{1\}, \{1, \sigma\}, \{1, \tau\}, \{1, \sigma\tau\}$

To find fixed field w.r.t. each subgroup

Since identity fixed every element of the field $Q(\sqrt{2},\sqrt{3})$
so fixed field w.r.t. $\{1\}$ is $Q(\sqrt{2},\sqrt{3})$

we have to find all elements in $Q(\sqrt{2},\sqrt{3})$ which fix by σ is $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

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

Compare coefficients we get $a=a, -b=b, c=c, d=-d$

So we get $b=0, d=0$ So fixed field is $Q(\sqrt{3})$

So fixed field w.r.t. $\{1,\sigma\}$ is $Q(\sqrt{3})$

we have to find all elements in $Q(\sqrt{2},\sqrt{3})$ which fix by τ is $\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

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

Compare coefficients we get $a=a, b=b, -c=c, d=-d$

So we get $c=0, d=0$ So fixed field is $Q(\sqrt{2})$

So fixed field w.r.t. $\{1,\tau\}$ is $Q(\sqrt{2})$

we have to find all elements in $Q(\sqrt{2},\sqrt{3})$ which fix by $\sigma\tau$ is $\sigma\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

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

Compare coefficients we get $a=a, -b=b, -c=c, d=d$

So we get $b=0, c=0$ So fixed field is $Q(\sqrt{6})$

So fixed field w.r.t. $\{1,\sigma\tau\}$ is $Q(\sqrt{6})$

And fixed field w.r.t. $\{1,\sigma,\tau,\sigma\tau\}$ is Q

subgroup	fixed field
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

(4)

The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is Galois of degree 6. The roots of this equation are $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ where $\rho = \zeta_3 = \dfrac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.

Hence the splitting field can be written $\mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2})$.

To determine the Galois group we use a more convenient set of generators, namely $\sqrt[3]{2}$ and ρ. Then any automorphism σ maps $\sqrt[3]{2}$ to one of $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ and maps ρ to ρ or $\rho^2 = \dfrac{-1-\sqrt{-3}}{2}$ since these are the roots of the cyclotomic polynomial $\Phi_3(x) = x^2 + x + 1$. Since σ is completely determined by its action on these two elements this gives only 6 possibilities and so each of these possibilities is actually an automorphism. To give these automorphisms explicitly, let σ and τ be the automorphisms defined by

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 = -1 - \rho. \end{cases}$$

basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho\sqrt[3]{2}, \rho(\sqrt[3]{2})^2\}$.

$$\begin{aligned} \sigma(\rho\sqrt[3]{2}) &= (\rho)(\rho\sqrt[3]{2}) = \rho^2\sqrt[3]{2} = (-1-\rho)\sqrt[3]{2} \\ &= -\sqrt[3]{2} - \rho\sqrt[3]{2} \end{aligned}$$

and we may similarly determine the action of σ on the other basis elements. This gives

$$\begin{aligned} \sigma : \quad & a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\rho + e\rho\sqrt[3]{2} + f\rho\sqrt[3]{4} \quad \longmapsto \\ & a - e\sqrt[3]{2} + (f-c)\sqrt[3]{4} + d\rho + (b-e)\rho\sqrt[3]{2} - c\rho\sqrt[3]{4}. \end{aligned}$$

The other elements of the Galois group are

$$1 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho^2 \sqrt[3]{2} \\ \rho \mapsto \rho \end{cases}$$

$$\tau\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho^2 \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases} \qquad \tau\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

Computing $\sigma\tau$ we have

$$\sigma\tau : \begin{cases} \sqrt[3]{2} \overset{\tau}{\mapsto} \sqrt[3]{2} \overset{\sigma}{\mapsto} \rho \sqrt[3]{2} \\ \rho \overset{\tau}{\mapsto} \rho^2 \overset{\sigma}{\mapsto} \rho^2 \end{cases}$$

i.e.,

$$\sigma\tau : \begin{cases} \sqrt[3]{2} \mapsto \rho \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

so that $\sigma\tau = \tau\sigma^2$. Similarly one computes that $\sigma^3 = \tau^2 = 1$.

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \tau\sigma\}$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$$

(5) the field $\mathbb{Q}(\sqrt[4]{2})$ is not Galois over $\mathbb{Q}$ since any automorphism is determined by where it sends $\sqrt[4]{2}$ and of the four possibilities $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, only two are elements of the field (the two real roots).

we have

$$\overbrace{\mathbb{Q} \underbrace{\subset \mathbb{Q}(\sqrt{2})}_{2} \subset \mathbb{Q}(\sqrt[4]{2})}^{4}$$

where $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are both Galois extensions

This shows that a Galois extension of a Galois extension

is not necessarily Galois.

Let τ be the map $\tau : \mathbb{C} \to \mathbb{C}$ defined by $\tau(a+bi) = a-bi$ (*complex conjugation*). Prove that τ is an automorphism of $\mathbb{C}$.

Solution: Let $\tau : C \to C$ defined by $\tau(a+bi) = a-bi$

To show τ is an automorphism

For one-one:

$\tau(a+bi) = \tau(c+di) \Rightarrow a-bi = c-di \Rightarrow a = c, b = d$

so $a+bi = c+di$

τ is one one map

since for every element $a+bi \in C$ we can find $a-bi \in C$ such that $\tau(a-bi) = a+bi$

So τ is onto. Now $\tau[(a+bi)+(c+di)] = \tau[(a+c)+(b+d)i] = (a+c)-(b+d)i = (a-bi)+(c-di) = \tau(a+bi)+\tau(c+di)$

$\tau[(a+bi)(c+di)] = \tau[(ac-bd)+(ad+bc)i] = (ac-bd)-(ad+bc)i = [(a-bi)(c-di)] = \tau(a+bi)\tau(c+di)$

So τ is homomorphism.

Hence τ is an automorphism.

Determine the fixed field of complex conjugation on $\mathbb{C}$.

To determine the fixed field for the complex conjugation that is for τ
to find $a + bi \in C$ such that $\tau(a + bi) = a + bi \Rightarrow a - bi = a + bi \Rightarrow a = a, b = -b$
$\Rightarrow b = 0$ so all elements in C such that $b = 0$ means fixed field is R that is set of real numbers.

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

To prove $Q(\sqrt{2})$ and $Q(\sqrt{3})$ are not isomorphic.
Suppose there is an isomorphism between this two field say $\phi : Q(\sqrt{2}) \to Q(\sqrt{3})$ defined by $\phi(a + b\sqrt{2} = a + b\sqrt{3})$
Since $\phi[(a + b\sqrt{2})(c + d\sqrt{2})] = \phi(a + b\sqrt{2})\phi(a + b\sqrt{2})$
$\Rightarrow \phi[(ac + 2bd) + (ad + bc)\sqrt{2}] = (a + b\sqrt{3})(c + d\sqrt{3})$
$\Rightarrow (ac + 2bd) + (ad + bc)\sqrt{3} = (ac + 3bd) + (ad + bc)\sqrt{3}$
Compairing the coefficient we get $ac + 2bd = ac + 3bd$
$\Rightarrow 2bd = 3bd \Rightarrow 2 = 3$
Which is not possible hence $Q(\sqrt{2})$ and $Q(\sqrt{3})$ are not isomorphic.

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

To determine the automorphisms of $Q(2^{\frac{1}{4}})$ over $Q(\sqrt{2})$
Since the polynomial which satisfied by $2^{\frac{1}{4}}$ over $Q(\sqrt{2})$ is $x^2 - \sqrt{2}$
so the degree of extension $[Q(2^{\frac{1}{4}}) : Q(\sqrt{2}) = 2]$
So we have 2 automorphism since the roots of the minimal polynomial is $\pm 2^{\frac{1}{4}}$
So possible mappings are $2^{\frac{1}{4}} \to 2^{\frac{1}{4}}$
and $2^{\frac{1}{4}} \to -2^{\frac{1}{4}}$
So $Gal(Q(2^{\frac{1}{4}}) : Q(\sqrt{2})) = \{1, \sigma\}$

THE FUNDAMENTAL THEOREM OF GALOIS THEORY

Definition. A *character*[1] χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L:

$$\chi : G \to L^{\times}$$

i.e., $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$ and $\chi(g)$ is a nonzero element of L for all $g \in G$.

Definition. The characters $\chi_1, \chi_2, \ldots, \chi_n$ of G are said to be *linearly independent* over L if they are linearly independent as functions on G, i.e., if there is no nontrivial relation

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0 \qquad (a_1, \ldots, a_n \in L \text{ not all } 0)$$

as a function on G (that is, $a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0$ for all $g \in G$).

Theorem

(Linear Independence of Characters) If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G with values in L then they are linearly independent over L.

Proof: Suppose the characters were linearly dependent. Among all the linear dependence relations (2) above, choose one with the minimal number m of nonzero coefficients a_i. We may suppose (by renumbering, if necessary) that the m nonzero coefficients are $a_1, a_2, \ldots, a_m$:

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_m\chi_m = 0.$$

Then for any $g \in G$ we have

$$a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_m\chi_m(g) = 0.$$

Let g_0 be an element with $\chi_1(g_0) \neq \chi_m(g_0)$ (which exists, since $\chi_1 \neq \chi_m$).

for every element of G, in particular we have

$$a_1\chi_1(g_0g) + a_2\chi_2(g_0g) + \cdots + a_m\chi_m(g_0g) = 0$$

i.e.,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0. \qquad (4$$

Multiplying equation (3) by $\chi_m(g_0)$ and subtracting from equation (4) we obtain

$$[\chi_m(g_0) - \chi_1(g_0)]a_1\chi_1(g) + [\chi_m(g_0) - \chi_2(g_0)]a_2\chi_2(g) + \cdots + [\chi_m(g_0) - \chi_{m-1}(g_0)]a_{m-1}\chi_{m-1}(g) = 0,$$

which holds for all $g \in G$. But the first coefficient is nonzero and this is a relation with fewer nonzero coefficients, a contradiction.

Corollary

If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular distinct automorphisms of a field K are linearly independent as functions on K.

Corollary Let K/F be any finite extension. Then

$$|\mathrm{Aut}(K/F)| \leq [K : F]$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Put another way, K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof: Let F_1 be the fixed field of $\mathrm{Aut}(K/F)$, so that

$$F \subseteq F_1 \subseteq K.$$

$[K : F_1] = |\mathrm{Aut}(K/F)|$. Hence $[K : F] = |\mathrm{Aut}(K/F)|[F_1 : F]$,

Corollary

Let G be a finite subgroup of automorphisms of a field K and let F be the fixed field. Then every automorphism of K fixing F is contained in G, i.e., $\mathrm{Aut}(K/F) = G$, so that K/F is Galois, with Galois group G.

Proof: By definition F is fixed by all the elements of G so we have $G \leq \mathrm{Aut}(K/F)$

$$\text{Hence } |G| \leq |\mathrm{Aut}(K/F)|.$$

$|G| = [K : F]$ and by the previous corollary $|\mathrm{Aut}(K/F)| \leq [K : F]$. This gives

$$[K : F] = |G| \leq |\mathrm{Aut}(K/F)| \leq [K : F]$$

Corollary

If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K then their fixed fields are also distinct.

Proof: Suppose F_1 is the fixed field of G_1 and F_2 is the fixed field of G_2. If $F_1 = F_2$ then by definition F_1 is fixed by G_2. By the previous corollary any automorphism fixing F_1 is contained in G_1, hence $G_2 \leq G_1$. Similarly $G_1 \leq G_2$ and so $G_1 = G_2$.

Definition. Let K/F be a Galois extension. If $\alpha \in K$ the elements $\sigma\alpha$ for σ in $\mathrm{Gal}(K/F)$ are called the *conjugates* (or *Galois conjugates*) of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the *conjugate field* of E over F.

Finally, notice that we now have 4 characterizations of Galois extensions K/F:

(1) splitting fields of separable polynomials over F

(2) fields where F is precisely the set of elements fixed by $\mathrm{Aut}(K/F)$ (in general, the fixed field may be larger than F)

(3) fields with $[K : F] = |\mathrm{Aut}(K/F)|$ (the original definition)

(4) finite, normal and separable extensions.

Theorem *(Fundamental Theorem of Galois Theory)*

Let K/F be a Galois extension

and set $G = \mathrm{Gal}(K/F)$. Then there is a bijection

$$\left\{\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array}\right\}$$

$$\left\{\begin{array}{c}\text{subfields } E \\ \text{of } K \\ \text{containing } F\end{array}\right\} \qquad \left\{\begin{array}{c}\text{subgroups } H \\ \text{of } G\end{array}\right\}$$

given by the correspondences

$$E \longrightarrow \left\{\begin{array}{c}\text{the elements of } G \\ \text{fixing } E\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{the fixed field} \\ \text{of } H\end{array}\right\} \longleftarrow H$$

which are inverse to each other.

Under this correspondence,

(1) (inclusion reversing) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$

(2) $[K : E] = |H|$ and $[E : F] = |G : H|$, the index of H in G:

$$\begin{array}{lll} K & & \\ | & \} & |H| \\ E & & \\ | & \} & |G : H| \\ F & & \end{array}$$

(3) K/E is always Galois, with Galois group $\mathrm{Gal}(K/E) = H$:

$$\begin{array}{ll} K & \\ | & H \\ E & \end{array}$$

(4) E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group

$$\mathrm{Gal}(E/F) \cong G/H.$$

More generally, even if H is not necessarily normal in G, the isomorphisms of E (into a fixed algebraic closure of F containing K) which fix F are in one to one correspondence with the cosets $\{\sigma H\}$ of H in G.

(5) If E_1, E_2 correspond to H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence the lattice of subfields of K containing F and the lattice of subgroups of G are "dual" (the lattice diagram for one is the lattice diagram for the other turned upside down).

Proof: Since for any subgroup H of G we have a unique fixed field as for distinct subgroups we have distinct fixed fields. so there is an injection from right to left that is from subgroups to subfields

Now to show there is correspondence between subfields and subgroups.
As K/F is Galois so we can say that K is splitting field of a separable polynomial $f(x) \in F[x]$. Let E be a subfield of K containing F so $f(x) \in E[x]$ then K is a splitting field of $f(x)$ over E so the extension K/E is Galois so E is a fixed field of $Aut(K/E) \leq G$ this implies that every subfield of K containing F arises as the fixed field for some subgroup of G
Hence there is bijection between subgroups and subfields

To prove 1) if E_1 is a fixed field of H_1 and E_2 is a fixed field of H_2. Suppose $E_1 \subset E_2$ to show $H_2 \leq H_1$ As both are groups so we need to show that $H_2 \subset H_1$ Let $\sigma \in H_2$ since σ fixes every element of E_2 so it fixes E_1 so $\sigma \in H_1$ therefore $H_2 \leq H_1$ Now suppose $H_2 \leq H_1$. Let $\alpha \in E_1$ and since $\sigma(\alpha) = \alpha$ for all $\sigma \in H_1$ since $H_2 \leq H_1$ so $\sigma(\alpha) = \alpha$ for all $\sigma \in H_2$

Since E_2 is a fixed field of H_2 so $\alpha \in E_2$
Hence $E_2 \subset E_1$.

To prove 2) Let E be a fixed field with respect to a subgroup H since $[K : E] = |H|$ and as K/F is Galois with Galois group G so $[K : F] = |G|$
since $[K : F] = [K : E][E : F] \Rightarrow |G| = |H|[E : F]$
$\Rightarrow [E : F] = \frac{|G|}{|H|} = |G : H| =$ index of H in G.

To prove 4) First we will show there is one to one correspondence between embedding of E and automorphisms of K
Let $\sigma \in Gal(K/F)$ and consider $\sigma|_E$ with the subfield $\sigma(E)$ of K. Conversely suppose $\tau : E \to \tau(E)$ be any embedding of E which fixes F. since if $\alpha \in E$ has $m_\alpha(x)$ be a minimal polynomial for α over F then $\tau(\alpha)$ is also root of $m_\alpha(x)$
Since K contains all the roots of $m_\alpha(x)$ so $\tau(\alpha) \in K$ hence $\tau(E) \subset K$
As K is a splitting field of a polynomial $f(x) \in F$ since $\tau(f(x)) = f(x)$ as τ fixes every element of F.
hence K is a splitting field for $\tau(f(x))$ also.
So we can extend τ to σ as
So every embedding of E is of the form $\sigma|_E$ for some $\sigma \in G$.
Now consider two automorphisms $\sigma, \sigma' \in G$ restrict to the same embedding τ of E fixing F if and only if $\sigma^{-1}\sigma'$ is the identity map (Since $\sigma^{-1}\sigma' = I \Rightarrow \sigma\sigma^{-1}\sigma' = \sigma I \Rightarrow \sigma' = \sigma$)
Since H is a subgroup so H contains identity element so $I \in H$ that is $\sigma^{-1}\sigma' \in H \Rightarrow \sigma' \in \sigma H$
So distinct embeddings of G are in bijection with cosets of H in G
Since number of cosets of H in G is $[G : H]$ and $[G : H] = [E : F]$

so $|Emb(E/F)| = [G : H] = [E : F]$
The extension E/F is Galois if and only if $|Aut(E/F)| = [E : F]$
This is possible if and only if every embedding is automorphism of E if and only if $\sigma(E) = E, \forall \sigma \in G$
Since $\sigma(E)$ is a subfield of K so there is a subgroup of G which fixes this field.
Since $\sigma(\alpha) \in \sigma(E)$ then $(\sigma h \sigma^{-1})(\sigma\alpha) = (\sigma h)(\sigma^{-1}\sigma)(\alpha) = (\sigma h)(\alpha) = \sigma(h\alpha) = \sigma\alpha, \forall h \in H$,Since H fixes elements of E
So $\sigma H \sigma^{-1}$ fixes $\sigma(E)$
Since E and $\sigma(E)$ are isomorphic so $[K : E] = [K : \sigma(E)]$ but $[K : E] = |H|$
and $[K : \sigma(E)] = |\sigma H \sigma^{-1}|$ so $|H| = |\sigma H \sigma^{-1}|$
Since we have to show that $\sigma H \sigma^{-1} = H$
Since two subfields are equal if and only if there fixed fields are equal that is $\sigma(E) = E$ if and only if $\sigma H \sigma^{-1}$ that is E is Galois over F if and only if H is normal in G.
Since automorphisms are one to one corresponding to cosets of H in G
as H is normal in G so automorphisms are one to one corresponds to elements in G/H
That is $Gal(E/F) \equiv G/H$

To prove 5) Let H_1 and H_2 are subgroups of G fixing the subfield E_1 and E_2 respectively.
Since any element in $H_1 \cap H_2$ fixes both E_1 as well as E_2 so it fixes every element of composite field E_1E_2 and conversely if σ fixes every elements of E_1E_2 so σ fixes E_1 so $\sigma \in H_1$ and similarly σ fixes every element of E_2 so $\sigma \in H_2$ so $\sigma \in H_1 \cap H_2$

FINITE FIELDS

Finite Fields Since a finite field has characteristic p so it is a finite dimensional vector space that is if $[F : F_p] = n$ then F has precisely p^n elements. Since then F is isomorphic to a splitting field of a polynomial $x^{p^n} - x$ so it is unique up to isomorphism.
Notation: For a finite field of order p^n is F_{p^n}

Proposition: Any finite field is isomorphic to F_{p^n} for some prime p and for some integer $n \geq 1$.The field F_{p^n} is the splitting field over F_p of the polynomial $x^{p^n} - x$, with the cyclic Galois group of order n generated by Frobenious automorphism σ_p. The subfield of F_{p^n} are all Galois over F_p and are in one to one correspondence with the divisors d of n. they are the fields F_{p^d}, the fixed field of σ_p^d

Proof: Since by definition, finite field has characteristic p so it is finite dimensional vector space over F_p that is $[F : F_p] = n$ so $|F| = p^n$ so any finite field is isomorphic to F_{p^n}. SInce F_{p^n} is a splitting field of the polynomial $x^{p^n} - x$
Consider Frobenius map $\sigma_p : F_{p^n} \to F_{p^n}$ defined by $\sigma_p(a) = a^p$
Since Frobenius map is isomorphism so here σ_p is automorphism. Since $[F_{p^n} : F] = n$ and if we find out the powers of σ_p the we have $\sigma_p^n = 1$ as $a^{p^n} = 1$ sa we have n elements in the Galois group that is $Gal(F_{p^n}/F_p) = \{\sigma_p, \sigma_p^2, ..., \sigma_p^n = 1\}$

so this is a cyclic group generated by σ_p

$Gal(F_{p^n}/F_p) =< \sigma_p > \approx Z_n$

Since every subgroup of a cyclic group is normal. and subgroups are corresponding to the divisors of n in Z_n so so for every divisor d of n there is precisely one subfield of F_{p^n} of order d that is F_{p^d} since order of subgroup is d so degree of extension w.r.t. this subgroup is also d

As every subgroup is normal so every subfield is Galois

Corollary: The irreducible polynomial $x^4 + 1Z[x]$ is reducible modulo every prime p

Proof: Consider the polynomial $x^4 + 1$ over F_p for the prime p.
For $p = 2$, $x^4 + 1 = (x + 1)^4$ so the polynomial is reducible.
Assume that p is odd. Then $p^2 - 1$ is divisible by 8
Since $p \equiv 1, 3, 5, 7 mod(8)$ then $p^2 \equiv 1 mod 8$ that is $8|p^2 - 1$
So $x^8 - 1|x^{p^2-1} - 1$. Since $x^8 - 1 = (x^4 - 1)(x^4 + 1)$
So $x^4 + 1|x^8 - 1|x^{p^2-1} - 1|x^{p^2} - x$ so $x^4 + 1|x^{p^2} - x$
Since the roots of the polynomial $x^{p^2} - x$ are in the field F_{p^2}
So extension generated by any root of $x^4 + 1$ is atmost of degree 2 over F_p

which means $x^4 + 1$ cannot be irreducible over F_p

Proposition

The polynomial $x^{p^n} - x$ is precisely the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all divisors of n.

Proof: Since F_{p^n} is a splitting field of a polynomial $x^{p^n} - x$
Let $p(x)$ be any irreducible polynomial of degree d , dividing $x^{p^n} - x$
If α is a root of $p(x)$ then the extension $F_p(\alpha)$ is a subfield of F_{p^n} of degree d so d is a divisor of n in this way we can find $x^{p^n} - x$ is the product of all distinct irreducible polynomial.

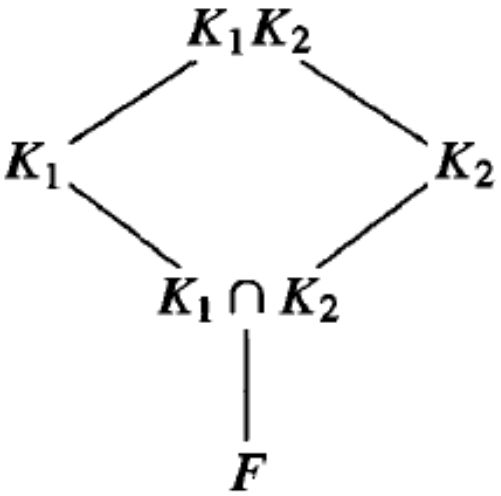
Proposition Let K_1 and K_2 be Galois extensions of a field F. Then

(1) The intersection $K_1 \cap K_2$ is Galois over F.

(2) The composite K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

of the direct product $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ are equal.



Proof: 1) Suppose $p(x)$ is an irreducible polynomial in $F[x]$ with a root $\alpha \in K_1 \cap K_2$.
So $\alpha \in K_1$ since K_1/F is Galois so every root of $p(x)$ is in K_1 similarly $\alpha \in K_2$ since K_2/F is Galois so every root of $p(x)$ is in K_2
hence every root of $p(x)$ is in $K_1 \cap K_2$.

So $K_1 \cap K_2$ is Galois over F.

2) Suppose K_1 is the splitting field of a separable polynomial $f_1(x)$ and K_2 is the splitting field of a separable polynomial $f_2(x)$ then composite field is the splitting field of the squarefree part of the polynomial $f_1(x)f_2(x)$ (separable polynomial). So K_1K_2 is Galois over F.
Consider the map $\phi : Gal(K_1K_2/F) \to Gal(K_1/F) \times Gal(K_2/F)$
$\phi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$
Homomorphism: $\phi(\sigma\tau) = (\sigma\tau|_{K_1}, \sigma\tau|_{K_2})$
$\phi(\sigma\tau) = (\sigma|_{K_1}\tau|_{K_1}, \sigma|_{K_2}\tau|_{K_2})$
$\phi(\sigma\tau) = (\sigma|_{K_1}, \sigma|_{K_2})(\tau|_{K_1}, \tau|_{K_2}) = \phi(\sigma)\phi(\tau)$
Injective: $ker(\phi) = \{\sigma \in Gal(K_1K_2)/F \ |\phi(\sigma) = 1\}$
$ker(\phi) = \{\sigma \in Gal(K_1K_2)/F | (\sigma|_{K_1}, \sigma|_{K_2}) = (1, 1)\}$
So Kernel of ϕ consists of all mapping which are identity on K_1 as well as K_2 so identity on K_1K_2
hence $Ker(\phi) = \{1\}$ So ϕ is injective.
Now let H be a subgroup of $Gal(K_1/F) \times Gal(K_2/F)$ which contains the images of ϕ
Since $(\sigma|_{K_1})|_{K_1 \cap K_2} = \sigma|_{K_1 \cap K_2} = (\sigma|_{K_2})|_{K_1 \cap K_2}$
we want to calculate order of H since H contains the images of ϕ that is all σ such that $(\sigma|_{K_1}, \sigma_{K_2})$
So we want to find number of tuples like (σ, τ) such that restriction on $K_1 \cap K_2$ are equal

since for every $\sigma \in Gal(K_1/F)$ we have the elements in $Gal(K_2/K_1 \cap K_2)$ which satisfies above condition.
So $|H| = |Gal(K_1/F)||Gal(K_2/K_1 \cap K_2)|$
Since $[K_2 : F] = [K_2 : K_1 \cap K_2][K_1 \cap K_2 : F]$
so $|Gal(K_2/F)| = |Gal(K_2/K_1 \cap K_2)||Gal(K_1/F)|$
Hence $|H| = |Gal(K_1/F)|\frac{Gak(K_2/F)}{Gal(K_1 \cap K_2/F)}|$
Since $[K_1K_2/F] = \frac{[K_2:F][K_2:F]}{[K_1 \cap K_2/F]}$
So $|H| = [K_1K_2/F]$
So images of ϕ is H which is $Gal(K_1K_2/F)$

Corollary

Let K_1 and K_2 be Galois extensions of a field F with $K_1 \cap K_2 = F$.

Then

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Conversely, if K is Galois over F and $G = \mathrm{Gal}(K/F) = G_1 \times G_2$ is the direct product of two subgroups G_1 and G_2, then K is the composite of two Galois extensions K_1 and K_2 of F with $K_1 \cap K_2 = F$.

Proof: The first part follows immediately from the proposition. For the second, let K_1 be the fixed field of $G_1 \subset G$ and let K_2 be the fixed field of $G_2 \subset G$. Then $K_1 \cap K_2$ is the field corresponding to the subgroup G_1G_2, which is all of G in this case, so $K_1 \cap K_2 = F$. The composite K_1K_2 is the field corresponding to the subgroup $G_1 \cap G_2$, which is the identity here, so $K_1K_2 = K$, completing the proof.

Corollary

Let E/F be any finite separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K.

Proof: There exists a Galois extension of F containing E, for example the composite of the splitting fields of the minimal polynomials for a basis for E over F (which are all separable since E is separable over F). Then the intersection of all the Galois extensions of F containing E is the field K.

Definition. The Galois extension K of F containing E in the previous corollary is called the *Galois closure* of E over F.

Proposition

Let K/F be a finite extension. Then $K = F(\theta)$ if and only if there exist only finitely many subfields of K containing F.

Proof: Suppose first that $K = F(\theta)$ is simple. Let E be a subfield of K containing F: $F \subseteq E \subseteq K$. Let $f(x) \in F[x]$ be the minimal polynomial for θ over F and let $g(x) \in E[x]$ be the minimal polynomial for θ over E. Then $g(x)$ divides $f(x)$ in $E[x]$. Let E' be the field generated over F by the coefficients of $g(x)$. Then $E' \subseteq E$ and clearly the minimal polynomial for θ over E' is still $g(x)$. But then

$$[K : E] = \deg g(x) = [K : E']$$

implies that $E = E'$. It follows that the subfields of K containing F are the subfields generated by the coefficients of the monic factors of $f(x)$, hence there are finitely many such subfields.

Suppose conversely that there are finitely many subfields of K containing F. If F is a finite field, then we have already seen that K is a simple extension (Proposition 17). Hence we may suppose F is infinite. It clearly suffices to show that $F(\alpha, \beta)$ is generated by a single element since K is finitely generated over F. Consider the subfields

$$F(\alpha + c\beta), \qquad c \in F.$$

Then since there are infinitely many choices for $c \in F$ and only finitely many such subfields, there exist c, c' in F, $c \neq c'$, with

$$F(\alpha + c\beta) = F(\alpha + c'\beta).$$

Then $\alpha + c\beta$ and $\alpha + c'\beta$ both lie in $F(\alpha + c\beta)$, and taking their difference shows that $(c - c')\beta \in F(\alpha + c\beta)$ Hence $\beta \in F(\alpha + c\beta)$ and then also $\alpha \in F(\alpha + c\beta)$. Therefore $F(\alpha, \beta) \subseteq F(\alpha + c\beta)$ and since the reverse inclusion is obvious, we have

$$F(\alpha, \beta) = F(\alpha + c\beta),$$

completing the proof.

Theorem

(The Primitive Element Theorem) If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.

Proof: Let L be the Galois closure of K over F. Then any subfield of K containing F corresponds to a subgroup of the Galois group $\mathrm{Gal}(L/F)$ by the Fundamental Theorem. Since there are only finitely many such subgroups, the previous proposition shows that K/F is simple. The last statement follows since any finite extension of fields in characteristic 0 is separable.

CYCLOTOMIC EXTENSIONS AND ABELIAN EXTENSIONS OVER Q

Since **cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is a Galois extension of $\mathbb{Q}$ of degree $\varphi(n)$ where φ denotes the Euler φ-function. Any automorphism of this field is uniquely determined by its action on the primitive n^{th} root of unity ζ_n**

Consider two groups Z_n and μ_n. If we define a function between this two groups say $\phi : Z_n \to \mu_n$ by $\phi(a) = (\xi_n)^a$ where ξ_n is primitive *nth* root of unity then ϕ is an isomorphism.

Since if $\phi(a) = \phi(b) \Rightarrow (\xi)^a = (\xi)^b \Rightarrow a = b$ then ϕ is one one function. since both are finite group so ϕ is onto. Now $\phi(a+b) = (\xi)^{a+b} = (\xi)^a(\xi)^b$ so it is homomorphism. Hence ϕ is an isomorphism.

Since there are precisely $\varphi(n)$
such integers a it follows that in fact each of these maps is indeed an automorphism of

$\mathbb{Q}(\zeta_n)$.

Theorem

The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is

isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is given explicitly by the map

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \pmod n &\longmapsto \sigma_a \end{aligned}$$

where σ_a is the automorphism defined by

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

Since σ_a is an automorphism

Homomorphism

$$(\sigma_a\sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^b)^a$$
$$= \zeta_n^{ab}$$

which shows that $\sigma_a\sigma_b = \sigma_{ab}$.

we know that every Galois automorphism is of the form σ_a for a uniquely defined a (mod n). Hence the map is an isomorphism.

Corollary

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the decomposition of the positive integer n into distinct prime powers. Then the cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1, 2, \ldots, k$ intersect only in the field $\mathbb{Q}$ and their composite is the cyclotomic field $\mathbb{Q}(\zeta_n)$. We have

Proof

Suppose that $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the decomposition of n into distinct prime powers. Since $\zeta_n^{p_2^{a_2} \cdots p_k^{a_k}}$ is a primitive $p_1^{a_1}$-th root of unity, the field $K_1 = \mathbb{Q}(\zeta_{p_1^{a_1}})$ is a subfield of $\mathbb{Q}(\zeta_n)$. Similarly, each of the fields $K_i = \mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1, 2, \ldots, k$ is a subfield of $\mathbb{Q}(\zeta_n)$. The composite of the fields contains the product $\zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \cdots \zeta_{p_k^{a_k}}$, which is a primitive n^{th} root of unity, hence the composite field is $\mathbb{Q}(\zeta_n)$. Since the extension degrees $[K_i : \mathbb{Q}]$ equal $\varphi(p_i^{a_i})$, $i = 1, 2, \ldots, k$ and $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k})$, the degree of the composite of the fields K_i is precisely the product of the degrees of the K_i.

Since the intersection of all these fields are Q

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2^{a_2}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$$

By above theorem

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$

Definition. The extension K/F is called an *abelian* extension if K/F is Galois and $\mathrm{Gal}(K/F)$ is an abelian group.

GALOIS GROUPS OF POLYNOMIALS

If K is a Galois extension of F then K is the splitting field for some separable polynomial $f(x)$ over F. Any automorphism $\sigma \in \mathrm{Gal}(K/F)$ maps a root of an irreducible factor of $f(x)$ to another root of the irreducible factor and σ is uniquely determined by its action on these roots (since they generate K over F). If we fix a labelling of the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$ we see that any $\sigma \in \mathrm{Gal}(K/F)$ defines a unique permutation of $\alpha_1, \ldots, \alpha_n$, hence defines a unique permutation of the subscripts $\{1, 2, \ldots, n\}$ (which depends on the fixed labelling of the roots). This gives an injection

$$\mathrm{Gal}(K/F) \hookrightarrow S_n$$

(1) Consider the biquadratic extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, which is the splitting field of $(x^2-2)(x^2-3)$. Label the roots as $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$ and $\alpha_4 = -\sqrt{3}$. The elements of the Galois group are $\{1, \sigma, \tau, \sigma\tau\}$ where σ maps $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$ and τ fixes $\sqrt{2}$ and maps $\sqrt{3}$ to $-\sqrt{3}$. As permutations of the roots for this labelling we see that σ interchanges the first two and fixes the second two and τ fixes the first two and interchanges the second two, i.e.,

$$\sigma = (12) \qquad \text{and} \qquad \tau = (34)$$

as elements of S_4. Similarly, or by taking the product of these two elements, we see that

$$\sigma\tau = (12)(34) \in S_4.$$

Hence

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \{1, (12), (34), (12)(34)\} \subset S_4$$

(2) The Galois group of $x^3 - 2$ acts as permutations on the three roots $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$ and $\rho^2\sqrt[3]{2}$ where ρ is a primitive 3^{rd} root of unity. With this ordering, the generators σ and τ we have defined earlier give the permutations

$$\sigma = (123) \qquad \tau = (23)$$

which gives

$$\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} = \{1, (123), (132), (23), (13), (12)\} = S_3,$$

in this case the full symmetric group on 3 letters.

Definition. Let $x_1, x_2, \ldots, x_n$ be indeterminates. The *elementary symmetric functions* $s_1, s_2, \ldots, s_n$ are defined by

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2 \cdots x_n
\end{aligned}
$$

Definition. The *general polynomial of degree n* is the polynomial

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$

whose roots are the indeterminates $x_1, x_2, \ldots, x_n$.

Since

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

(1) The expression $(x_1 - x_2)^2$ is symmetric in x_1, x_2. We have

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = s_1^2 - 4s_2,$$

a polynomial in the elementary symmetric functions.

(2) The polynomial $x_1^2 + x_2^2 + x_3^2$ is symmetric in x_1, x_2, x_3, and in this case we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) \\ &= s_1^2 - 2s_2. \end{aligned}$$

(3) The polynomial $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$ is symmetric. Since

$$\begin{aligned} (x_1x_2 + x_1x_3 + x_2x_3)^2 &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2(x_1^2x_2x_3 + x_2^2x_1x_3 + x_3^2x_1x_2) \\ &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2x_1x_2x_3(x_1 + x_2 + x_3) \end{aligned}$$

we have

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = s_2^2 - 2s_1s_3.$$

Definition. Define the *discriminant* D of $x_1, x_2, \ldots, x_n$ by the formula

$$D = \prod_{i<j} (x_i - x_j)^2.$$

If the roots of the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ are $\alpha_1, \alpha_2, \ldots, \alpha_n$, then the discriminant of $f(x)$ is[2]

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Note:

The Galois group of $f(x) \in F[x]$ is a subgroup of A_n if and only if the discriminant $D \in F$ is the square of an element of F.

Polynomials of Degree 2

Note that this restates results we obtained previously by explicitly solving for the roots: if the polynomial is reducible (namely D is a square in F), then the Galois group is trivial (the splitting field is just F), while if the polynomial is irreducible the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ since the splitting field is the quadratic extension $F(\sqrt{D})$.

Consider the polynomial $x^2 + ax + b$ with roots α, β.

$$D = s_1^2 - 4s_2 = (-a)^2 - 4(b) = a^2 - 4b,$$

Polynomials of degree 3

Suppose the cubic polynomial is

$$f(x) = x^3 + ax^2 + bx + c.$$

If we make the substitution $x = y - a/3$ the polynomial becomes

$$g(y) = y^3 + py + q$$

where

$$p = \frac{1}{3}(3b - a^2) \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

$$D = -4p^3 - 27q^2.$$

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$$

(Galois Group of a Cubic)

a. If the cubic polynomial $f(x)$ is reducible, then it splits either into three linear factors or into a linear factor and an irreducible quadratic. In the first case the Galois group is trivial and in the second case the Galois group is of order 2.

b. If the cubic polynomial $f(x)$ is irreducible then a root of $f(x)$ generates an extension of degree 3 over F, so the degree of the splitting field over F is divisible by 3. Since the Galois group is a subgroup of S_3, there are only two possibilities, namely A_3 or S_3. The Galois group is A_3 (i.e., cyclic of order 3) if and only if the discriminant D is a square.

Polynomials of Degree 4

Let the quartic polynomial be

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

which under the substitution $x = y - a/4$ becomes the quartic

$$g(y) = y^4 + py^2 + qy + r$$

with

$$p = \frac{1}{8}(-3a^2 + 8b)$$

$$q = \frac{1}{8}(a^3 - 4ab + 8c)$$

$$r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d).$$

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$$

$$\begin{aligned} D = &- 128b^2d^2 - 4a^3c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 \\ &+ 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d \\ &+ 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd. \end{aligned}$$

(Galois group of a quartic)

If D is not a square, then $G = S_4$.

D is a square, then $G = A_4$.