

(a) L/\mathbb{Q} is a Galois extension if

$$[L:\mathbb{Q}] = |\text{Aut}_{\mathbb{Q}}(L)|$$

(b) Let L/K be a Galois extension then

i) There is a 1-1 correspondence between subgroups of $\text{Aut}_K(L)$ and subfields $K \subseteq M \subseteq L$.

ii). $[L:M] = |\text{Aut}_M(L)|$
and $[M:K] = |\text{Aut}_K(L) / \text{Aut}_M(L)|$.

iii) M/K is normal if and only if $\text{Aut}_M(L) \triangleleft \text{Aut}_K(L)$

In this case $\text{Aut}_K(M) \cong \text{Aut}_K(L) / \text{Aut}_M(L)$.

(c) L' $L' = \mathbb{Q}(\sqrt[4]{2})$

|

L $L = \mathbb{Q}(\sqrt{2})$

|

\mathbb{Q}

L/\mathbb{Q} is the splitting field of $x^2 - 2$, L'/L is the splitting field of $x^2 - \sqrt{2}$.

However $x^4 - 2$ has 1 root in
 $\mathbb{Q}(\sqrt[4]{2})$ but $i\sqrt[4]{2} \notin L$

So not normal.

2d) L_1/\mathbb{Q} , L_2/\mathbb{Q} Galois.

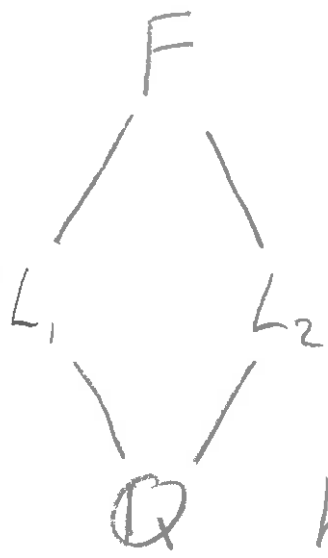
Let $F = \mathbb{Q}(L_1, L_2)$.

L_1 is normal so splitting field
of some polynomial $f(x)$.

L_2 is normal so splitting field
of some polynomial $g(x)$.

So $f(x)g(x)$ splits in F
and in fact is the smallest field where
this happens

So F/\mathbb{Q} is normal and separable
(all extensions over \mathbb{Q}
are separable)
So is a Galois extension.



There are 2 functions

$$\varphi_i: \text{Aut}_{\mathbb{Q}}(F) \rightarrow \text{Aut}_{\mathbb{Q}}(L_i) \quad *$$

Thus we define a homomorphism.

$$\varphi: \text{Aut}_{\mathbb{Q}}(F) \rightarrow \text{Aut}_{\mathbb{Q}}(L_1) \times \text{Aut}_{\mathbb{Q}}(L_2)$$

$$\varphi(g) = (\varphi_1(g), \varphi_2(g))$$

This is a homomorphism

* given by restricting the automorphism to L_i .

Suppose that $\varphi(g) = (e, e)$

i.e. g fixes L_1 , and fixes L_2

then since every element of F is obtained from elements of L_1 and L_2 then we see that g is the identity

2) Suppose M/\mathbb{Q} is a Galois extension
so normal i.e. if $f(x)$ has a root in M
all roots are in M .

Suppose $f(z) = 0$ for $z \in M$

then $\overline{f(z)} = f(\bar{z}) = 0$ so $\bar{z} \in M$.

Since thus $z \mapsto \bar{z}$ is a field
isomorphism with fixed field
 $M \cap \mathbb{R}$

This is not the identity if $M \cap \mathbb{R} \neq \emptyset$

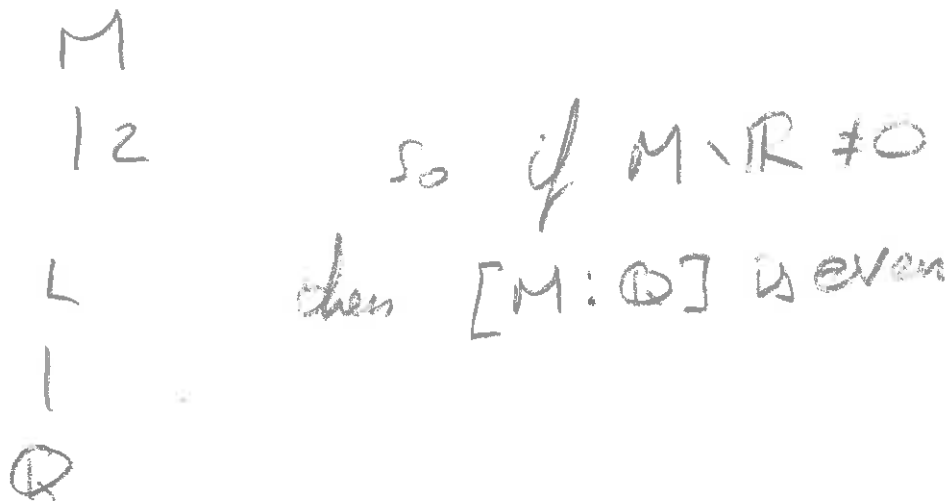
In this case we have an

isomorphism of order 2.

Thus we get a field.

$L = M \cap \mathbb{R}$ the fixed field of
Complex conjugation

Thus we obtain a field diagram



3a). $\text{Aut}_K(L) = \left\{ \sigma: L \rightarrow L \mid \sigma(k) = k \forall k \in K \right\}$

See 1b)

3b) $x^n - \theta$ has roots

$0 \leq k < n$ $e^{k2\pi i/n} \sqrt[n]{\theta}$ since $x^n - 1$ splits

we see that $M(\sqrt[n]{\theta}) = L$

Any Automorphism is determined
by $\sqrt[n]{\theta}$

Let k be the smallest integer such that there is an element

$$\sigma \in \text{Aut}_m(L) \text{ s.t.}$$

$$\sigma(\sqrt[m]{\theta}) = e^{2\pi i k/n} \sqrt[m]{\theta}$$

Claim Any Automorphism is σ^l for some l .

Note that $\sigma^l(\sqrt[m]{\theta}) = e^{2\pi i k l/n} \sqrt[m]{\theta}$
 thus if φ there is φ not of the form σ^l , then

$$\varphi(\sqrt[m]{\theta}) = e^{2\pi i m/n} \sqrt[m]{\theta}$$

where $m \neq kl$ for any l .

but then let a be such that

$$m - ka < k.$$

$$\text{then } \sigma^{-a} \varphi(\sqrt[m]{\theta}) = \sigma^{-a} (e^{2\pi i m/n} \sqrt[m]{\theta})$$

$$= e^{2\pi i (m - ka)/n} \sqrt[m]{\theta}$$

but this contradicts minimality of k

Thus $\text{Aut}_m(L)$ is cyclic
generated by σ

$$\text{also } o(\sigma) = \frac{n}{k}$$

$$\text{So } |\text{Aut}_m(L)| \mid n$$

4a) Suppose $\alpha^k \in \mathbb{Q}$ for some
~~block~~. Suppose. ~~then~~ ~~fast~~.

~~then~~
Suppose that k is the minimal $k > 0$
s.t. $\alpha^k \in \mathbb{Q}$. Suppose $k \nmid m$.

then there is an a s.t. $m - ka < k$.
then $\alpha^{m-ka} \in \mathbb{Q}$ since \mathbb{Q} is a
field. Thus $m - ka = 0$ by minimality
of k . So $k \mid m$ but ~~then~~ m is prime
So $k = 1$, or m so $k = m$ since
 $\alpha \notin \mathbb{Q}$.

b) The roots of $x^m - \alpha^m$ are

$$e^{2\pi i k/m} \alpha, \quad 0 \leq k < m.$$

Suppose that one of the subproducts

is in \mathbb{Q}

$$\text{Then } \prod_{i=1}^k \alpha_i \in \mathbb{Q}.$$

~~However~~ let $\alpha_i = e^{2\pi i k_i/m} \alpha$

$$\text{So } \prod_{i=1}^k \alpha_i = e^{2\pi i (\sum k_i)/m} \alpha^k$$

So if this is rational we have

$$e^{2\pi i (\sum k_i)/m} = \pm 1 \quad \text{and thus}$$

$$\alpha^k \in \mathbb{Q} \implies \alpha \in \mathbb{Q}$$

4d) Since $(x^n - \alpha^n) = \prod_{i=1}^n (x - \alpha_i)$.

then if this is reducible one of the polynomials $\prod_{j=1}^k (x - \alpha_{i_j})$.

is in $\mathbb{Q}[x]$

~~$\Rightarrow \mathbb{Q} \subseteq \mathbb{C}$~~ . So $[F(\alpha); F] = n$
since $x^n - \alpha^n$ is
irred.

4e) ~~Any Automorphism.~~

$F(\alpha)$ is the splitting field of $x^n - \alpha^n$

so is Galois. and $|\text{Aut}_F(F(\alpha))| = n$.

Also any automorphism φ is determined by $\varphi(\alpha)$ which is a root of $x^n - \alpha^n$.

also since there are n such automorphisms any of these is possible

Thus this group is generated by
 $\varphi: F(\alpha) \rightarrow F(\alpha)$. given by

$$\varphi(\alpha) = e^{2\pi i/n} \alpha.$$