1a) $L/\mathbb{Q}$ is a Galois extension if

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

1b) Let L/K be a Galois extension then

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

ii) $[L:M] = |\mathrm{Aut}_M(L)|$

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

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

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

1c)

$$\begin{array}{c} L' \\ | \\ L \\ | \\ \mathbb{Q} \end{array}$$

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

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

$L/\mathbb{Q}$ 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 ~~E~~ $F = \mathbb{Q}(L_1, L_2)$

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 seperable (all extensions over $\mathbb{Q}$ are seperable)

So is a Galois extension.

$$\begin{tikzcd}[column sep=small] & F \arrow[dl, dash] \arrow[dr, dash] & \\ L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

There are 2 functions

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

Thus we define a homomorphism.

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

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

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 $M \setminus \mathbb{R} \neq \emptyset$

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

$$\begin{array}{c} M \\ \Big| \, 2 \\ L \\ \Big| \\ \mathbb{Q} \end{array}$$

So if $M \setminus \mathbb{R} \neq \emptyset$ then $[M:\mathbb{Q}]$ is even

3a). $Aut_K(L) = \{ \sigma : L \to L \mid \sigma(k) = k \ \forall k \in K \}$

See 1b)

3b) $x^n - \theta$ has roots $e^{k 2\pi i/n} \sqrt[n]{\theta}$ $0 \le k < n$ since $x^n - 1$ splits

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

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

Let k be the smallest integer such that there is an element $\sigma \in Aut_M(L)$ s.t.

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

Claim Any Automorphism is σ^l for some l.

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

thus if ~~θ~~ there is φ not of the form σ^l, then

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

where $m \neq kl$ for any l.

but then let ~~b~~ a be such that

~~b~~ $\quad m - ka < k$.

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

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

but this contradicts minimality of k

Thus $Aut_M(L)$ is cyclic generated by σ

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

So $|Aut_M(L)| \mid n$

---

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

~~$0<k<m$.~~ ~~suppose.~~ ~~then $\exists a$ s.t.~~

~~[illegible]~~

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

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 $k|m$ 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

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

Suppose that one of the subproducts is in $\mathbb{Q}$

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

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

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

So if this is rational we have

$e^{2\pi i (\Sigma k_i)/m} = \pm 1$ and then

$\alpha^k \in \mathbb{Q}$ $\Rightarrow\!\Leftarrow$

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

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

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

$\Rightarrow\Leftarrow$ to c). So $[F(\alpha) : F] = n$ since $x^n - \alpha^n$ is irred.

4e). ~~Any Automorphism~~ $x^n - \alpha^n$

$F(\alpha)$ is the splitting field of

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

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 $\varphi : F(\alpha) \to F(\alpha)$ given by

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