THE FUNDAMENTAL THEOREM OF GALOIS THEORY: Let L/F be a finite Galois extension. There is a bijection

$$\begin{array}{ccc} \{\text{fields } E \mid F \subseteq E \subseteq L\} & \longleftrightarrow & \{\text{subgroups } H \leq \mathrm{Gal}(L/F)\} \\ E & \mapsto & \mathrm{Gal}(L/E) \\ L^H & \hookleftarrow & H \end{array}$$

Moreover, this bijective correspondence enjoys the following properties:

(1) $\overset{\mathrm{Gal}(L/\star)}{\longrightarrow}$ and $\overset{L^\star}{\longleftarrow}$ each reverse the order of inclusion:
$E \subseteq E' \iff \mathrm{Gal}(L/E') \leq \mathrm{Gal}(L/E)$; equivalently
$L^H \subseteq L^{H'} \iff H' \leq H$.

(2) $\overset{\mathrm{Gal}(L/\star)}{\longrightarrow}$ and $\overset{L^\star}{\longleftarrow}$ convert between degrees of extensions and indices of subgroups:
$[E : F] = [\mathrm{Gal}(L/F) : \mathrm{Gal}(L/E)]$; equivalently
$[\mathrm{Gal}(L/F) : H] = [L^H : F]$.

(3) Normal subgroups correspond to intermediate fields that are Galois over F:
E/F is Galois if and only if $\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/F)$; equivalently
$N \trianglelefteq G$ if and only if L^N/F is Galois.
In this case, $\mathrm{Gal}(E/F) = \mathrm{Gal}(L/F)/\mathrm{Gal}(L/E)$.

(1) Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. From earlier work, we know that:

- $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$.
- $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$, with $\sigma \begin{bmatrix} \sqrt[3]{2} \\ \omega \end{bmatrix} = \begin{bmatrix} \omega\sqrt[3]{2} \\ \omega \end{bmatrix}$ and $\tau \begin{bmatrix} \sqrt[3]{2} \\ \omega \end{bmatrix} = \begin{bmatrix} \sqrt[3]{2} \\ \omega^2 \end{bmatrix}$.
- $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ via $\sigma \mapsto (1\,2\,3)$ and $\tau \mapsto (2\,3)$.

(a) List all subgroups of S_3, and draw a diagram indicating which is contained in which.

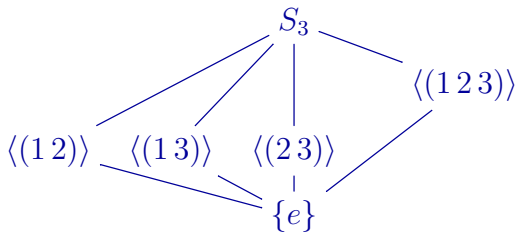
(b) Use the previous part and the Fundamental Theorem to determine how many[1] intermediate fields E are between $\mathbb{Q}$ and L. Then draw a diagram to indicate containments among the fields.

(c) Compute the index of each subgroup of S_3. Use this and the Fundamental Theorem to determine $[E : \mathbb{Q}]$ for each intermediate field E.

(d) Determine which subgroups of S_3 are normal. Use this and the Fundamental Theorem to determine which intermediate fields are Galois over $\mathbb{Q}$.

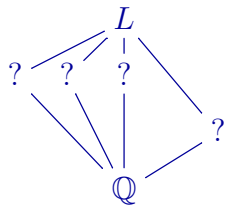
(e) Explicitly identify the intermediate fields E.

(a)

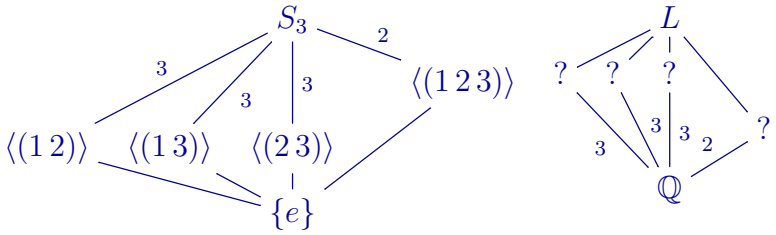


[1] Do *not* explicitly identify the fields yet; just make up a placeholder name for each intermediate field E.

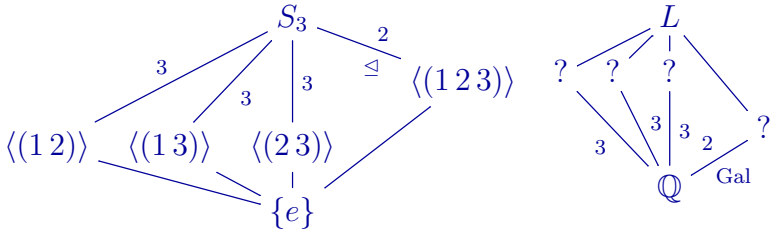
(b) Four:



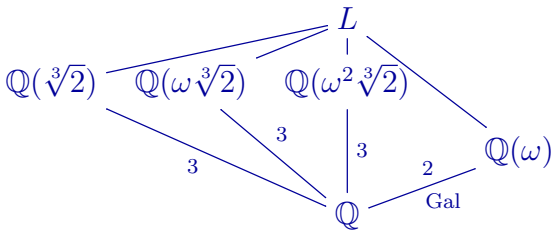
(c)



(d)



(e)



(2) Let L/F be a finite Galois extension.

(a) When is every intermediate field $E \subseteq L$ Galois over F?

(b) If $[L : F] = n$ and $n = p^e m$ for some prime p and positive integer m that is not a multiple of p, explain why there exists an intermediate field E with $[E : F] = m$.

(a) If and only if every subgroups is normal. This happens, for example, if G is abelian.

(b) Let $G = \mathrm{Gal}(L/F)$. Then by the Sylow Theorems, there is a subgroup $H \leq G$ of order p^e. Then $m = [G : H] = [L^H : F]$, so $E = L^H$ works.

(3) Proof[2] of Fundamental Theorem:

(a) Show that the maps $\overset{\mathrm{Gal}(L/\star)}{\longrightarrow}$ and $\overset{L^\star}{\longleftarrow}$ give the bijection as stated in the Theorem.

(b) Prove part (1) of The Fundamental Theorem of Galois Theory.

(c) Prove part (2) of The Fundamental Theorem of Galois Theory.

[2]Hint: Use Artin's Theorem and its Corollaries generously!

(a) First, we note that these are well-defined: for $E \subseteq L$, L/E is indeed Galois by a Corollary of Artin's Theorem, and $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/F)$. Also, for $H \subseteq G$, L^H is a subfield of L by an exercise, and L^H contains F since every element of H fixes F.
Let $F \subseteq E \subseteq L$. Then E maps to $\mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/F)$. By a Corollary of Artin's Theorem, we have $L^{\mathrm{Gal}(L/E)} = E$. This shows that one composition is the identity.
Let $H \leq \mathrm{Gal}(L/F)$. Then H maps to L^H. This maps to $\mathrm{Aut}(L/L^H)$ which is H by Artin's Theorem. This shows that the other composition is the identity.

(b) This follows from the definitions: if $E \subseteq E'$, then any automorphism that fixes E' definitely fixes E, so $\mathrm{Gal}(L/E') \leq \mathrm{Gal}(L/E)$. For the converse, we write $E = L^H$ and $E' = L^{H'}$; if $H' \leq H$, then anything fixed by all elements of H is fixed by all elements of H', so $E = L^H \subseteq L^{H'} = E'$.

(c) By definition of Galois, we have $[L : F] = |\mathrm{Gal}(L/F)|$. Since L/E is also Galois, we have $[L : E] = |\mathrm{Gal}(L/E)|$. Then

$$[E : F] = \frac{[L : F]}{[L : E]} = \frac{|\mathrm{Gal}(L/F)|}{|\mathrm{Gal}(L/E)|} = [\mathrm{Gal}(L/F) : \mathrm{Gal}(L/E)].$$