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: Given any subgroup H of G we obtain a unique fixed field $E = K_H$ by Corollary 12. This shows that the correspondence above is injective from right to left.

If K is the splitting field of the separable polynomial $f(x) \in F[x]$ then we may also view $f(x)$ as an element of $E[x]$ for any subfield E of K containing F. Then K is also the splitting field of $f(x)$ over E, so the extension K/E is Galois. By Corollary 10, E is the fixed field of $\mathrm{Aut}(K/E) \leq G$, showing that *every* subfield of K containing F arises as the fixed field for some subgroup of G. Hence the correspondence above is surjective from right to left, hence a bijection. The correspondences are inverse to each other since the automorphisms fixing E are precisely $\mathrm{Aut}(K/E)$ by Corollary 10.

We have already seen that the Galois correspondence is inclusion reversing in Proposition 4, which gives (1).

If $E = K_H$ is the fixed field of H, then Theorem 9 gives $[K : E] = |H|$ and $[K : F] = |G|$. Taking the quotient gives $[E : F] = |G : H|$, which proves (2).

Corollary 11 gives (3) immediately.

Suppose $E = K_H$ is the fixed field of the subgroup H. Every $\sigma \in G = \mathrm{Gal}(K/F)$ when restricted to E is an embedding $\sigma|_E$ of E with the subfield $\sigma(E)$ of K. Conversely, let $\tau : E \xrightarrow{\sim} \tau(E) \subseteq \overline{F}$ be any embedding of E (into a fixed algebraic closure $\overline{F}$ of F containing K) which fixes F. Then $\tau(E)$ is in fact contained in K: if $\alpha \in E$ has minimal polynomial $m_\alpha(x)$ over F then $\tau(\alpha)$ is another root of $m_\alpha(x)$ and K contains all these roots by Theorem 13. As above K is the splitting field of $f(x)$ over E and so also the splitting field of $\tau f(x)$ (which is the same as $f(x)$ since $f(x)$ has coefficients in F) over $\tau(E)$. Theorem 13.27 on extending isomorphisms then shows that we can extend τ to an isomorphism σ:

$$\begin{tikzcd}
\sigma : & K \arrow[r, "\sim"] \arrow[d, dash] & K \arrow[d, dash] \\
\tau : & E \arrow[r, "\sim"] & \tau(E).
\end{tikzcd}$$

Since σ fixes F (because τ does), it follows that *every* embedding τ of E fixing F is the restriction to E of some automorphism σ of K fixing F, in other words, every embedding of E is of the form $\sigma|_E$ for some $\sigma \in G$.

Two automorphisms $\sigma, \sigma' \in G$ restrict to the *same* embedding of E if and only if $\sigma^{-1}\sigma'$ is the identity map on E. But then $\sigma^{-1}\sigma' \in H$ (i.e., $\sigma' \in \sigma H$) since by (3) the automorphisms of K which fix E are precisely the elements in H. Hence the distinct embeddings of E are in bijection with the cosets σH of H in G. In particular this gives

$$|\mathrm{Emb}(E/F)| = [G : H] = [E : F]$$

where $\mathrm{Emb}(E/F)$ denotes the set of embeddings of E (into a fixed algebraic closure of F) which fix F. Note that $\mathrm{Emb}(E/F)$ contains the automorphisms $\mathrm{Aut}(E/F)$.

The extension E/F will be Galois if and only if $|\mathrm{Aut}(E/F)| = [E : F]$. By the equality above, this will be the case if and only if each of the *embeddings* of E is actually an *automorphism* of E, i.e., if and only if $\sigma(E) = E$ for every $\sigma \in G$.

If $\sigma \in G$, then the subgroup of G fixing the field $\sigma(E)$ is the group $\sigma H \sigma^{-1}$, i.e.,

$$\sigma(E) = K_{\sigma H \sigma^{-1}}.$$

To see this observe that if $\sigma\alpha \in \sigma(E)$ then

$$(\sigma h \sigma^{-1})(\sigma\alpha) = \sigma(h\alpha) = \sigma\alpha \qquad \text{for all } h \in H,$$

since h fixes $\alpha \in E$, which shows that $\sigma H \sigma^{-1}$ fixes $\sigma(E)$. The group fixing $\sigma(E)$ has order equal to the degree of K over $\sigma(E)$. But this is the same as the degree of K over E since the fields are isomorphic, hence the same as the order of H. Hence $\sigma H \sigma^{-1}$ is precisely the group fixing $\sigma(E)$ since we have shown containment and their orders are the same.

Because of the bijective nature of the Galois correspondence already proved we know that two subfields of K containing F are equal if and only if their fixing subgroups are equal in G. Hence $\sigma(E) = E$ for all $\sigma \in G$ if and only if $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, in other words E is Galois over F if and only if H is a normal subgroup of G.

We have already identified the embeddings of E over F as the set of cosets of H in G and when H is normal in G seen that the embeddings are automorphisms. It follows that in this case the *group* of cosets G/H is identified with the *group* of automorphisms of the Galois extension E/F by the definition of the group operation (composition of automorphisms). Hence $G/H \cong \text{Gal}(E/F)$ when H is normal in G, which completes the proof of (4).

Suppose H_1 is the subgroup of elements of G fixing the subfield E_1 and H_2 is the subgroup of elements of G fixing the subfield E_2. Any element in $H_1 \cap H_2$ fixes both E_1 and E_2, hence fixes every element in the composite E_1E_2, since the elements in this field are algebraic combinations of the elements of E_1 and E_2. Conversely, if an automorphism σ fixes the composite E_1E_2 then in particular σ fixes E_1, i.e., $\sigma \in H_1$, and σ fixes E_2, i.e., $\sigma \in H_2$, hence $\sigma \in H_1 \cap H_2$. This proves that the composite E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Similarly, the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2, completing the proof of the theorem.

Example: ($\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{2}, \rho)$)

We have already seen examples of this theorem at the beginning of this section. We now see that the diagrams of subfields for the two fields $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{2}, \rho)$ given before indicate *all* the subfields for these two fields.

Since every subgroup of the Klein 4-group is normal, all the subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are Galois extensions of $\mathbb{Q}$.

Similarly, since the only nontrivial normal subgroup of S_3 is the subgroup of order 3, we see that only the subfield $\mathbb{Q}(\rho)$ of $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$ is Galois over $\mathbb{Q}$, with Galois group isomorphic to $S_3/\langle \sigma \rangle$, i.e., the cyclic group of order 2. For example, the nontrivial automorphism of $\mathbb{Q}(\rho)$ is induced by restricting any element (τ, for instance) in the nontrivial coset of $\langle \sigma \rangle$ to $\mathbb{Q}(\rho)$. This is clear from the explicit descriptions of these automorphisms given before — each of the elements τ, $\tau\sigma$, $\tau\sigma^2$ in this coset map ρ to ρ^2. The restrictions of the elements of $\text{Gal}(K/\mathbb{Q})$ to the (non-Galois) cubic subfields do not give automorphisms of these fields in general, rather giving isomorphisms of these fields with each other, in accordance with (4) of the theorem.

Example: ($\mathbb{Q}(\sqrt{2} + \sqrt{3})$)

Consider the field $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. This is clearly a subfield of the Galois extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The other roots of the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ are therefore the distinct conjugates of $\sqrt{2}+\sqrt{3}$ under the Galois group. The conjugates are

$$\pm\sqrt{2}\pm\sqrt{3}$$

which are easily seen to be distinct. The minimal polynomial is therefore

$$[x-(\sqrt{2}+\sqrt{3})][x-(\sqrt{2}-\sqrt{3})][x-(-\sqrt{2}+\sqrt{3})][x-(-\sqrt{2}-\sqrt{3})]$$

which is quickly computed to be the polynomial x^4-10x^2+1. It follows that this polynomial is irreducible and that

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

either by degree considerations or by noting that only the automorphism 1 of $\{1,\sigma,\tau,\sigma\tau\}$ fixes $\sqrt{2}+\sqrt{3}$ so the fixing group for this field is the same as for $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Example: (Splitting Field of x^8-2)

The splitting field of x^8-2 over $\mathbb{Q}$ is generated by $\theta=\sqrt[8]{2}$ (any fixed 8th root of 2, say the real one) and a primitive 8th root of unity $\zeta=\zeta_8$. Recall from Section 13.6 that

$$\mathbb{Q}(\zeta_8)=\mathbb{Q}(i,\sqrt{2}).$$

Since $\theta^4=\sqrt{2}$ we see that the splitting field is generated by θ and i. The subfield $\mathbb{Q}(\theta)$ is of degree 8 over $\mathbb{Q}$ (since x^8-2 is irreducible, being Eisenstein), and all the elements of this field are real. Hence $i\notin\mathbb{Q}(\theta)$ and since i generates at most a quadratic extension of this field, the splitting field

$$\mathbb{Q}(\sqrt[8]{2},\zeta_8)=\mathbb{Q}(\sqrt[8]{2},i)$$

is of degree 16 over $\mathbb{Q}$.

The Galois group is determined by the action on the generators θ and i which gives the possibilities

$$\begin{cases}\theta\mapsto\zeta^a\theta & a=0,1,2,\dots,7\\ i\mapsto\pm i\end{cases}$$

Since we have already seen that the degree of the extension is 16 and there are only 16 possible such maps, it follows that in fact each of the maps above is an automorphism of $\mathbb{Q}(\sqrt[8]{2},i)$ over $\mathbb{Q}$.

Define the two automorphisms

$$\sigma:\begin{cases}\theta\mapsto\zeta\theta\\ i\mapsto i\end{cases}\qquad\qquad \tau:\begin{cases}\theta\mapsto\theta\\ i\mapsto -i\end{cases}$$

(τ is the map induced by complex conjugation). Since

$$\begin{aligned}\zeta=\zeta_8&=\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}=\frac{1}{2}(1+i)\sqrt{2}\\ &=\frac{1}{2}(1+i)\theta^4\end{aligned}$$

we can easily compute what happens to ζ from the explicit expressions for the powers of ζ in the following Figure 1.

Using these explicit values we find

$$\sigma:\begin{cases}\theta\mapsto\zeta\theta\\ i\mapsto i\\ \zeta\mapsto-\zeta=\zeta^5\end{cases}\qquad\qquad \tau:\begin{cases}\theta\mapsto\theta\\ i\mapsto -i\\ \zeta\mapsto\zeta^7\end{cases}$$

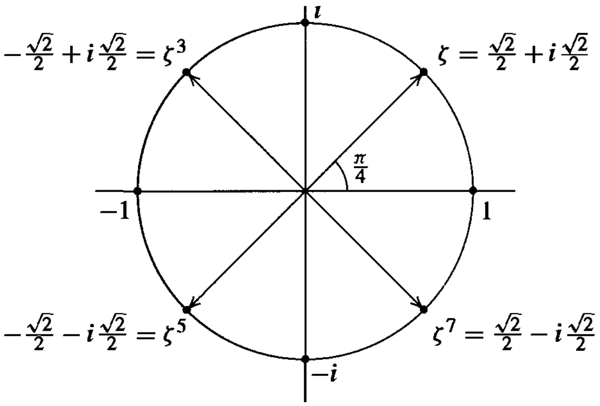
i
$-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}=\zeta^3$
$\zeta=\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$
$\frac{\pi}{4}$
-1
1
$-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}=\zeta^5$
$\zeta^7=\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$
$-i$

Fig. 1

Note that the reason we are interested in also keeping track of the action on the element ζ is that it will be needed in computing the composites of automorphisms, for example in computing

$$\begin{aligned}\sigma^2(\theta) &= \sigma(\zeta\theta) = \sigma(\zeta)\sigma(\theta) = (-\zeta)(\zeta\theta) = -\zeta^2\theta \\ &= -i\theta.\end{aligned}$$

We can similarly compute the following automorphisms:

$$\sigma : \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto i \\ \zeta \mapsto \zeta^5 \end{cases} \qquad \tau\sigma : \begin{cases} \theta \mapsto \zeta^7\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\sigma^2 : \begin{cases} \theta \mapsto \zeta^6\theta \\ i \mapsto i \\ \zeta \mapsto \zeta \end{cases} \qquad \tau\sigma^2 : \begin{cases} \theta \mapsto \zeta^2\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$$\sigma^3 : \begin{cases} \theta \mapsto \zeta^7\theta \\ i \mapsto i \\ \zeta \mapsto -\zeta \end{cases} \qquad \tau\sigma^3 : \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\sigma^4 : \begin{cases} \theta \mapsto -\theta \\ i \mapsto i \\ \zeta \mapsto \zeta \end{cases} \qquad \tau\sigma^4 : \begin{cases} \theta \mapsto -\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$$\sigma^5 : \begin{cases} \theta \mapsto \zeta^5\theta \\ i \mapsto i \\ \zeta \mapsto -\zeta \end{cases} \qquad \tau\sigma^5 : \begin{cases} \theta \mapsto \zeta^3\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\sigma^6 : \begin{cases} \theta \mapsto \zeta^2\theta \\ i \mapsto i \\ \zeta \mapsto \zeta \end{cases} \qquad \tau\sigma^6 : \begin{cases} \theta \mapsto \zeta^6\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$