Example 46.5, we saw that for $\sigma \in G(K/\mathbb{Q})$ given by complex conjugation, $\lambda(\mathbb{Q}(\sqrt[3]{2})) = \langle\sigma\rangle$. Therefore,

$$K_{\langle\sigma\rangle} = \mathbb{Q}(\sqrt[3]{2}).$$

Theorem 46.4 says that

$$(G(K/\mathbb{Q}) : \langle\sigma\rangle) = (G(K/\mathbb{Q}) : \lambda(\mathbb{Q}(\sqrt[3]{2})) = [\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3.$$

Since $|\langle\sigma\rangle| = 2$,

$$|G(K/\mathbb{Q})| = (G(K/\mathbb{Q}) : \langle\sigma\rangle) \cdot |\langle\sigma\rangle| = 6. \qquad \blacktriangle$$

46.8 Theorem Let K be a normal extension of a field F and E an intermediate field of the extension. Then E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. Furthermore, if E is a normal extension of F, then $G(E/F)$ is isomorphic with $G(K/F)/G(K/E)$.

Proof We first assume that E is a normal extension of F. Let $\tau \in \lambda(E) = G(K/E)$ and $\sigma \in G(K/F)$. We verify that $\sigma\tau\sigma^{-1} \in G(K/E)$ to show that $\lambda(E)$ is a normal subgroup of $G(K/F)$. By Theorem 44.11, σ^{-1} maps E isomorphically onto E. Therefore, for any $\alpha \in E$, $\tau(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha)$ and

$$\sigma\tau\sigma^{-1}(\alpha) = \sigma(\tau(\sigma^{-1}(\alpha))) = \sigma(\sigma^{-1}(\alpha)) = \alpha.$$

Thus, $\sigma\tau\sigma^{-1} \in G(K/E)$, and $\lambda(E)$ is a normal subgroup of $G(K/F)$.

We next assume that $\lambda(E)$ is a normal subgroup of $G(K/F)$ and show that E is a normal extension of F. We must show that E is a splitting field over F and that E is a separable extension of F. Theorem 45.8 says that the extension is separable. We use Corollary 44.14 to show that E is a splitting field over F. Let σ_1 be any isomorphism fixing F and mapping E onto a subfield of K. Let σ be an extension of σ_1 to an isomorphism from K onto K. Such an extension exists by the Isomorphism Extension Theorem 44.6. Let $\alpha \in E$ and $\tau \in \lambda(E)$. By assumption $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. Thus

$$\tau\sigma(\alpha) = \sigma(\alpha).$$

Since every $\tau \in \lambda(E)$ fixes $\sigma(\alpha)$, $\sigma(\alpha) \in K_{\lambda(E)}$. By Theorem 46.3, $\sigma(\alpha) \in E$. Thus the isomorphism σ_1 maps E isomorphically onto E. By Corollary 44.14, E is a splitting field over F, and therefore, E is a normal extension of F.

Assuming that E is a normal extension of F, we know that any isomorphism of K that fixes F maps E isomorphically onto itself. Using this fact, we can define $\phi : G(K/F) \to G(E/F)$ by simply letting $\phi(\sigma)$ be the map σ restricted to E. By the Isomorphism Extension Theorem 44.6, ϕ maps onto $G(E/F)$. Also

$$\text{Ker}(\phi) = \{\sigma \in G(K/F) \mid \sigma(\alpha) = \alpha \text{ for all } \alpha \in E\} = G(K/E).$$

Therefore $G(E/F)$ is isomorphic with

$$G(K/F)/\text{Ker}(\phi) = G(K/F)/G(K/E). \qquad \blacklozenge$$

46.9 Example Recall from Example 43.14, $x^3 - 2$ has only one zero in the field extension $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is not a splitting field, and therefore, not a normal extension. As we saw, the only automorphism of $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the identity map ι. So the set of automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ fixing $\mathbb{Q}(\sqrt[3]{2})$ is the same as the set of automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ fixing $\mathbb{Q}$. In the case of a normal extension, this could not happen since λ gives a one-to-one correspondence.

In Example 46.7, we saw that

$$|G(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q})| = 6.$$

Up to isomorphism, there are only two groups of order 6, $\mathbb{Z}_6$ and S_3. Since $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is not a normal extension of $\mathbb{Q}$, $\lambda(\mathbb{Q}(\sqrt[3]{2}))$ is not a normal subgroup of $G(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q})$. Every subgroup of $\mathbb{Z}_6$ is a normal subgroup, so $G(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q})$ is isomorphic with S_3. ▲

The next theorem completes the basic facts that are used to apply Galois theory to particular problems. The theorem is usually interpreted in terms of subgroup and subfield diagrams. It says that the diagram for subfields is the same as the diagram for the corresponding subgroups, except that the diagrams are inverted.

46.10 Theorem Let K be a normal extension of F, with E_1 and E_2 intermediate fields. Then

$$E_1 \text{ is a subfield of } E_2 \quad \text{if and only if} \quad \lambda(E_2) \text{ is a subgroup of } \lambda(E_1).$$

Proof Suppose that $E_1 \leq E_2$. Then any automorphism of K that fixes every element of E_2 clearly fixes every element of E_1, which means that $\lambda(E_2) \leq \lambda(E_1)$.

Now suppose that $\lambda(E_2) \leq \lambda(E_1)$. Let $\alpha \in K_{\lambda(E_1)}$. Then α is fixed by every element of $\lambda(E_1)$ and, therefore, by every element of $\lambda(E_2)$. So $\alpha \in K_{\lambda(E_2)}$. Thus

$$E_1 = K_{\lambda(E_1)} \leq K_{\lambda(E_2)} = E_2. \qquad ◆$$

46.11 Example As before, we let K be the splitting field for $f(x) = x^3 - 2$ over $\mathbb{Q}$. Each $\sigma \in G(K/\mathbb{Q})$ is completely determined by how σ permutes the zeros of $f(x)$. Since $f(x)$ has three zeros, $G(K/E)$ is isomorphic with a subgroup of the symmetric group S_3. As we saw in Example 46.9, $G(K/\mathbb{Q})$ is isomorphic with S_3. By labeling the zeros of $f(x)$ by

$$\begin{aligned} r_1 &= \sqrt[3]{2} \\ r_2 &= \frac{\sqrt[3]{2}}{2}\left(-1 + \sqrt{3}i\right) \\ r_3 &= \frac{\sqrt[3]{2}}{2}\left(-1 - \sqrt{3}i\right) \end{aligned}$$

the isomorphism $\phi : G(K/\mathbb{Q}) \to S_3$ can be defined by letting $\phi(\sigma)$ be the permutation of the zeros of $f(x)$ by the automorphism σ, that is, $\phi(\sigma)(i) = j$ if $\sigma(r_i) = r_j$. We will abuse notation slightly and identify elements in $G(K/\mathbb{Q})$ with their corresponding elements in the symmetric group S_3.

The subgroup diagram for S_3 is displayed in Figure 46.12 (a). By Theorem 46.10, the subfield diagram for K is given in Figure 46.12 (b).

The automorphism corresponding to the transposition $(2, 3)$ maps r_2 to r_3, maps r_3 to r_2, and fixes r_1, which is complex conjugation. As we saw in Example 46.7, $K_{\langle(2,3)\rangle} = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(r_1)$. The automorphism corresponding to $(1, 2)$ fixes r_3, maps r_1 to r_2, and maps r_2 to r_1. Thus $K_{\langle(1,2)\rangle} = \mathbb{Q}(r_3)$. Similarly, $K_{\langle(1,3)\rangle} = \mathbb{Q}(r_2)$.

We can determine $K_{\langle(1,2,3)\rangle}$ by noticing that

$$\begin{aligned} |\lambda(\mathbb{Q}(\sqrt{3}i))| &= [K : \mathbb{Q}(\sqrt{3}i)] \\ &= [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i) : \mathbb{Q}(\sqrt{3}i)] \\ &= [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i) : \mathbb{Q})]/[\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}] \\ &= 3. \end{aligned}$$

The subfield diagram shows that there is only one intermediate field E with $[K : E] = 3$, so $K_{\langle(1,2,3)\rangle} = \mathbb{Q}(\sqrt{3}i)$. Summarizing:

$$\begin{aligned} K_{\{\iota\}} &= K \\ K_{S_3} &= \mathbb{Q} \\ K_{\langle(2,3)\rangle} &= \mathbb{Q}(r_1) = \mathbb{Q}(\sqrt[3]{2}) \end{aligned}$$