Problem §5c Let $L = \mathbb{Q}(\sqrt{D})$ for some square-free integer D. Write down all elements in $\operatorname{Gal}_{\mathbb{Q}} L$, justifying your reasoning.

Solution: We have shown that $\sigma(a + b\sqrt{D}) = a \pm b\sqrt{D}$ are the only two possible automorphisms in $\operatorname{Gal}_{\mathbb{Q}} L$. The identity automorphism, $\sigma_I(a + b\sqrt{D}) = a + b\sqrt{D}$ is clearly an isomorphism; it remains to show that $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$ is an isomorphism.

Consider $a + b\sqrt{D}, c + d\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. Then

$$\begin{aligned}
\sigma((a + b\sqrt{D})(c + d\sqrt{D})) &= \sigma(ac + (ad + bc)\sqrt{D} + bdD) \\
&= (ac + bdD) - (ad + bc)\sqrt{D} \\
&= ac - ad\sqrt{D} - bd\sqrt{D} + bdD \\
&= (a - b\sqrt{D})(c - d\sqrt{D}) \\
&= \sigma(a + b\sqrt{D})\sigma(c + d\sqrt{D}).
\end{aligned}$$

Hence σ is a homomorphism.

Injectivity is clear; suppose

$$\sigma(a + b\sqrt{D}) = a - b\sqrt{D} = c - d\sqrt{D} = \sigma(c + d\sqrt{D})$$

for $a + b\sqrt{D}, c + d\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. Then clearly we need $a = c$, $b = d$.

Surjectivity is also clear; for any $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, simply choose $a - b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. Then

$$\sigma(a - b\sqrt{D}) = a + b\sqrt{D}.$$

Hence σ is an isomorphism.