Galois Theory solutions, #3.

1. We’ve seen that every element of \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) has the form \( a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \), where \( a, b, c, d \in \mathbb{Q} \) (Use the proof of the Tower Law). Let \( K \) be a subfield of \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). Then \( 1 \in K \) implies that \( \mathbb{Q} \in K \). So suppose that \( K \neq \mathbb{Q} \). It suffices to show that \( K \) contains \( \sqrt{2}, \sqrt{3}, \) or \( \sqrt{6} \) (because if, say, \( \sqrt{2} \in K \) then \( \mathbb{Q}(\sqrt{2}) \subset K \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) which implies by the Tower Law that \( K = \mathbb{Q}(\sqrt{2}) \) or \( K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). If not, then it must contain an element of the form \( x = b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \) where at least 2 of \( b, c, d \) are nonzero. Squaring this and subtracting a rational number, we get that \( y = 3cd\sqrt{2} + 2bd\sqrt{3} + bc\sqrt{6} \in K \). If exactly 2 of \( b, c, d \) are nonzero then \( y \) is a nonzero multiple of \( \sqrt{2}, \sqrt{3}, \) or \( \sqrt{6} \), a contradiction. If all are nonzero then \( x = y - (3cd/b)x = c\sqrt{3} + d\sqrt{6}, \) where \( c = (2b^2 - c^2)d/b \neq 0 \), and we may repeat the argument with \( x' \) in place of \( x \).

2. (a) Any \( \mathbb{Q} \)-automorphism of \( \mathbb{Q}(\sqrt{2}) \) sends \( \sqrt{2} \) to \( \pm\sqrt{2} \). So the Galois group consists of the identity automorphism and the automorphism \( a + b\sqrt{2} \mapsto a - b\sqrt{2} \).

(b) If \( \sigma \in \text{Gal}(\mathbb{Q}(\alpha) \supset \mathbb{Q}) \), then \( \sigma(\alpha) \) is a 5th root of \( 7 \), and real as it is contained in \( \mathbb{Q}(\alpha) \) which is contained in \( \mathbb{R} \). But there is a unique real 5-th root of \( 7 \), so \( \sigma(\alpha) = \alpha \). Because every element of \( \mathbb{Q}(\alpha) \) is a polynomial in \( \alpha \) it follows that the only element of the Galois group is the identity automorphism.

(c) \( \omega \) has minimal polynomial \( f = t^4 + t^3 + t^2 + t + 1 \) and the other zeroes of \( f \) in \( K(\omega) \) are \( \omega^2, \omega^3, \) and \( \omega^4 \). Any element of \( \sigma \in \text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q}) \) is determined by its value on \( \omega \), which by Lemma 48 must be one of the four zeroes of \( f \), and by (1.3) one actually gets a \( \sigma \) such that \( \sigma(\omega) = \omega^2 \). Then \( \sigma^2(\omega) = \omega^4, \sigma^3(\omega) = \omega^3, \) and \( \sigma^4(\omega) = \omega \), so the Galois group is a cyclic group of order 4.

(d) We have
\[
(\alpha^2)^3 + \alpha^2 + 1 = (\alpha^3)^2 + \alpha^2 + 1 = (\alpha^3 + \alpha + 1)^2 = 0
\]
and
\[
(\alpha^4)^3 + \alpha^4 + 1 = (\alpha^3)^4 + \alpha^4 + 1 = (\alpha^3 + \alpha + 1)^4 = 0,
\]
so the zeroes of \( t^4 + t + 1 \) in \( \mathbb{Z}_2(\alpha) \) are \( \alpha, \alpha^2, \) and \( \alpha^4 \). Any element of \( \sigma \in \text{Gal}(\mathbb{Z}_2(\alpha) \supset \mathbb{Z}_2) \) is determined by its value on \( \alpha \), which by Lemma 48 must be one of the zeroes of \( f \), and by (1.3) one actually gets \( \sigma \) and \( \tau \) such that \( \sigma(\alpha) = \alpha^2 \) and \( \tau(\alpha) = \alpha^4 \). So \( G = \{ id, \sigma, \tau \} \) has order 3 and therefore is cyclic.

1
3. We have

\[
(t - \text{id}(\sqrt{2} + \sqrt{3})) \left( t - \sigma_1(\sqrt{2} + \sqrt{3}) \right) \left( t - \sigma_2(\sqrt{2} + \sqrt{3}) \right) \left( t - \sigma_3(\sqrt{2} + \sqrt{3}) \right)
\]

\[
= \left( t \left( \sqrt{2} + \sqrt{3} \right) \right) \left( t - \left( -\sqrt{2} + \sqrt{3} \right) \right) \left( t - \left( \sqrt{2} - \sqrt{3} \right) \right) \left( t - \left( -\sqrt{2} - \sqrt{3} \right) \right)
\]

\[
= \left( t + (\sqrt{2} + \sqrt{3}) \right) \left( t - (\sqrt{2} + \sqrt{3}) \right) \left( t + (\sqrt{2} - \sqrt{3}) \right) \left( t - (\sqrt{2} - \sqrt{3}) \right)
\]

\[
= \left( t^2 - (5 + 2\sqrt{6}) \right) \left( t^2 - (5 - 2\sqrt{6}) \right)
\]

\[
= t^4 - 10t^2 + 1.
\]

This is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.