1. Section 14.6

2. (a) Factors as \( x^3 - x^2 - 4 = (x - 2)(x^2 + x + 2) \). Galois group is \( \mathbb{Z}/2\mathbb{Z} \).
(b) Factors as \( x^3 - 2x + 4 = (x + 2)(x^2 - 2x + 2) \). Galois group is \( \mathbb{Z}/2\mathbb{Z} \).
(c) Irreducible. (Rational root theorem implies only possible roots are \( \pm 1 \), easy to check these aren’t roots.) By equation (14.18),

\[
\text{Discriminant} = -4(-1)^3 - 27(1)^2 = -23.
\]

This is not a square, so the Galois group is \( S_3 \).
(d) Irreducible using same method as in (c). Calculate

\[
p = (-6 - 1)/3 = -7/3, \quad q = (2 + 18 - 27)/27 = 20/27.
\]

\[
\text{Discriminant} = -4(-7/3)^3 - 27(20/27)^2 = 36.
\]

This is a square, so Galois group is \( \mathbb{Z}/3\mathbb{Z} \).

9. First we show that the polynomial \( x^4 + 4x - 1 \) is irreducible. There are many ways to do this; here is one.

It is easy to check that \( \pm 1 \) are not roots, so the only possible factorization is into two quadratics. From the constant term, such a factorization would necessarily have the form \( x^4 + 4x - 1 = (x^2 + ax + 1)(x^2 + bx - 1) \). From the \( x \) coefficient we see that \( b - a = 4 \) and from the \( x^3 \) coefficient we see that \( a + b = 0 \). Hence \( b = 2 \) and \( a = -2 \). But then the \( x^2 \) coefficient on the right is \(-4\) rather than \( 4 \), so there is no such factorization. Therefore \( x^4 + 4x - 1 \) is irreducible.

From the formulas on page 614, the resolvent cubic is \( h(x) = x^3 + 4x + 16 \) and the discriminant is \( D = -27(4)^4 + 256(-1)^3 = -531697 \). Now \( h(x) \) factors as \( h(x) = (x + 2)(x^2 - 2x + 8) \). We therefore have \( G \cong D_8 \) or \( G \cong \mathbb{Z}/4\mathbb{Z} \). By #19(c), we see that \( G \cong \mathbb{Z}/4\mathbb{Z} \) is not possible since \( D < 0 \), so \( G \cong D_8 \).

18. Let \( \theta \) be a root of \( f(x) = x^3 - 3x + 1 \). The discriminant is \( D = -4(-3)^3 - 27(1)^2 = 81 \), which is a square, so the splitting field is \( \mathbb{Q}(\theta) \) and the Galois group is isomorphic to \( \mathbb{Z}/3\mathbb{Z} \).

Suppose our polynomial factors as \( f(x) = (x - \theta)(x - \alpha)(x - \beta) \). From the \( x^2 \) coefficient, we see that \( \alpha + \beta = -\theta \). Furthermore, the discriminant \( D \) satisfies

\[
\sqrt{D} = 9 = (\theta - \alpha)(\theta - \beta)(\alpha - \beta)
\]

for some ordering of \( \alpha, \beta \). Since \( f'(\theta) = (\theta - \alpha)(\theta - \beta) \), we obtain

\[
9 = (3\theta^2 - 3)(\alpha - \beta), \quad \text{hence} \quad \alpha - \beta = \frac{3}{\theta^2 - 1}.
\]

One method to calculate the inverse of \( \theta^2 - 1 \) is to use matrices. View \( K = \mathbb{Q}(\theta) \) as a 3-dimensional vector space over \( \mathbb{Q} \) with basis \( 1, \theta, \theta^2 \). The matrix for multiplication by \( \theta \), viewed as a \( \mathbb{Q} \)-linear transformation of \( K \), is given with respect to this basis as

\[
\theta : \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}
\]

Taking the square of this matrix and subtracting 1, we see that the matrix for multiplication by \( \theta^2 - 1 \) is

\[
\theta^2 - 1 : \begin{pmatrix} -1 & -1 & 0 \\ 0 & 2 & -1 \\ 1 & 0 & 2 \end{pmatrix}
\]
The inverse of this matrix times 3 is
\[
\frac{3}{\theta^2 - 1} \begin{pmatrix} -4 & -2 & -1 \\ 1 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix}.
\]

From the first column of this matrix, we see that \(\frac{3}{\theta^2 - 1} = -4 + \theta + 2\theta^2\). Now it is easy to solve the two linear equations
\[
\begin{align*}
\alpha + \beta &= -\theta \\
\alpha - \beta &= -4 + \theta + 2\theta^2.
\end{align*}
\]

We find \(\alpha = -2 + \theta^2\) and \(\beta = 2 - \theta - \theta^2\).

19. (a) Since \(\sqrt{D}\) is the product of the differences of the roots of \(f(x)\), and these roots lie in \(K\), it follows that \(\sqrt{D} \in K\).

(b) The element \(\tau\) has order 2, so \(\tau_K\) has order dividing 2, i.e. order 1 or 2. Now \(\tau_K\) has order 1 if and only if it is trivial, i.e. iff \(K\) is fixed by \(\tau\), i.e. if and only if \(K \subseteq \mathbb{R}\).

(c) Suppose that \(\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}\) and that \(D < 0\). Since \(\mathbb{Q}(\sqrt{D}) \subset K\) and \(\sqrt{D} \notin \mathbb{R}\), it follows from part (b) that \(\tau_K\) has order 2. However, a cyclic group of order 4 has a unique element of order 2, so \(\tau_K\) must be this element; and the fixed field will be the unique subfield of \(K\) of index 2, so this must be \(\mathbb{Q}(\sqrt{D})\). Therefore \(\tau_K\) fixes \(\mathbb{Q}(\sqrt{D})\). Yet \(D < 0\) implies that complex conjugation does not fix \(\sqrt{D}\), so this is a contradiction.

(d) This is the same argument. Let \(K\) be a cyclic quartic field, viewed as a subfield of \(\mathbb{C}\). Suppose that \(\mathbb{Q}(\sqrt{D}) \subset K\) with \(D < 0\). Complex conjugation is an order 2 element of \(\text{Gal}(K/\mathbb{Q})\) (it is nontrivial because it does not fix \(\sqrt{D}\), since \(D < 0\)), and hence its fixed field is the unique index 2 subfield of \(K\), namely \(\mathbb{Q}(\sqrt{D})\). This is a contradiction, since complex conjugation does not fix \(\sqrt{D}\).

References