§14.2, 11. We may suppose that \( f(x) \) is monic, and by Gauss’ lemma is irreducible. Therefore \( [K : \mathbb{Q}] = 4 \). Let \( L \) be the splitting field of \( f \), then \( L \supset K \) and it is given that \( G(L/\mathbb{Q}) = S_4 \). Then any proper subfield \( M \) of \( K \) should be a quadratic extension of \( \mathbb{Q} \). Then the subgroup corresponding to \( M \), under the fundamental theorem of Galois theory, is of index 2 and hence should be \( A_4 \). Then \( G(L/K) \) is a subgroup of \( A_4 \) of index 2 which is not possible. (See page 111, Fig 8.)

§14.2, 12. The roots of \( f(x) = x^4 - 14x^2 + 9 \) are \( \pm \alpha, \pm \beta \), where \( \alpha = \sqrt{7 + 2\sqrt{10}} \) and \( \beta = \sqrt{7 - 2\sqrt{10}} \). Then the discriminant of \( f(x) \) is \( 4\alpha\beta(\alpha^2 - \beta^2) = 4 \cdot 3 \cdot 16 \cdot 10 \) which is not a square in \( \mathbb{Q} \). Hence the Galois group of \( f(x) \) is \( S_4 \).

§14.3, 8. We have seen (in an earlier HW) that \( f(x) = x^p - x - a \) is irreducible and separable over \( \mathbb{F}_p \). If \( \alpha \) is a root of \( f(x) \), then so is \( \alpha + b, b = 1, 2, \cdots, p - 1 \). Thus \( \mathbb{F}_p(\alpha) \) is the splitting field of \( f(x) \) and its degree over \( \mathbb{F}_p \) is \( p \). We know that there is a Galois automorphism \( \sigma \) that maps \( \alpha \mapsto \alpha + 1 \). Then \( \sigma^i(\alpha) = \alpha + i, i = 1, 2, \cdots, p - 1 \). Moreover, for \( i \neq j \), \( \sigma^i \neq \sigma^j \), whence the Galois group of \( f(x) \) is a cyclic group generated by \( \sigma \).

§14.3, 9, 9]  

a. For any \( x \in \mathbb{F}_q \), since \( x^q - x = 0 \), we have \( \sigma_q(x) = x^{p^m} = x \).

b. Any finite extension of \( \mathbb{F}_q \) of degree \( n \) is a finite field of cardinality \( q^n = p^{mn} \). Hence, such an extension is the splitting field of \( x^{p^m} - x \) over \( \mathbb{F}_p \), and hence the splitting field of \( x^q - x \) over \( \mathbb{F}_q \). Thus any extension of degree \( n \) (over \( \mathbb{F}_q \)) is the finite field \( \mathbb{F}_{q^n} \).

c. It is clear that \( \sigma_q^n = 1 \) since \( x^{q^n} - x = 0 \) for all \( x \in \mathbb{F}_{q^n} \). No lesser power of \( \sigma_q \) can be identity, for if \( \sigma_q^i = 1, i < n \), then \( x^{q^i} - x = 0 \) for all \( x \in \mathbb{F}_{q^n} \) which is impossible since there are only \( q^i \) roots of this equation. Thus \( \mathbb{F}_{q^n} \) is a cyclic extension of \( \mathbb{F}_q \).

d. By the fundamental theorem of Galois theory subfields \( L, \mathbb{F}_q \subset L \subset \mathbb{F}_{q^n} \), are in bijective correspondence with subgroups of \( G = G(\mathbb{F}_{q^n}/\mathbb{F}_q) \). Since \( G \) is cyclic of order \( n \), these are in turn is in bijective correspondence with the divisors \( d \) of \( n \).
§14.6, 2a. The Galois group is cyclic of order 2.

§14.6, 2d. The Galois group is $A_3$. (One checks that the determinant is a square.)

§14.6, 11. We know that the order of the Galois group $G$ is $> 4$, and hence $G \simeq S_4, A_4$, or $D_8$.

§14.6, 13. We use the discussion in page 614-615 to do this problem. The roots of the resolvent cubic are $0, -(\alpha + \beta)^2, -(\alpha - \beta)^2$. In particular the resolvent cubic is reducible over $\mathbb{Q}$. We also have $f(x) = (x^2 - \alpha^2)(x^2 - \beta^2)$, $\alpha^2 + \beta^2 = -a$ and $\alpha^2 \beta^2 = b$. Further $D = 16\alpha^2 \beta^2(\alpha^2 - \beta^2)^4$.

a. This is a straightforward calculation. Check it yourself.

b(i). $G \simeq V$ if and only if the resolvent cubic is a product of linear factors. This is valid if and only if $\alpha \beta \in \mathbb{Q}$.

c(ii),(iii). We know that $G \simeq D_8$ or $C$ if and only if the resolvent cubic splits into a linear and a quadratic polynomial which is equivalent to $\alpha \beta \notin \mathbb{Q}$ (i.e. $b$ is not a square). Further the subgroup corresponding to $\mathbb{Q}(\sqrt{D}) \subset \text{spl}(f)$ is $G \cap A_4$. (Note that $D$ is not a square in $\mathbb{Q}$ if $G \simeq D_8$ or $C$, and we have $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\alpha \beta)$ in this case.) Moreover, in either cases, we see that $\mathbb{Q}(\alpha \beta)$ is the splitting field of the resolvent cubic since $\alpha^2 + \beta^2 = -a \in \mathbb{Q}$. Now, if $G \simeq C$ with generator $\sigma$, where $\sigma$ maps $\alpha \mapsto -\beta$ and $\beta \mapsto -\sigma$ since $\sigma(\alpha \beta) = -\alpha \beta$. Thus the element $\alpha \beta(\alpha^2 - \beta^2)$ is fixed by $\sigma$ and hence by $G$. This implies that $\alpha \beta(\alpha^2 - \beta^2) \in \mathbb{Q}$, or in other words $b(a^2 - 4b)$ is a square. If $G \simeq D_8$, let $\tau$ be the automorphism that maps $\alpha \mapsto \beta$. Then in fact $G = \{< \sigma, \tau >; \sigma^4 = \tau = 1; \sigma \tau = \tau \sigma^3\}$. But $\tau$ doesn’t fix $\alpha \beta(\alpha^2 - \beta^2)$, and therefore $b(a^2 - 4b)$ is not a square.