GALOIS THEORY ANSWERS TO CHAPTER 3 EXERCISES

Exercises 3.1

1. Let τ be any automorphism of $\mathbb{Q}(\sqrt{2})$. By Proposition 3.1, τ is a $\mathbb{Q}$-automorphism.

   $(\tau(\sqrt{2}))^2 = \tau((\sqrt{2})^2) = \tau(2) = 2$, so $\tau(\sqrt{2}) = \pm\sqrt{2}$.

   τ is determined by its effect on the basis $\{1, \sqrt{2}\}$ for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Clearly $\tau(1) = 1$, so the two possibilities for τ are the identity ι, which is certainly an automorphism, and σ which is shown to be an automorphism in Example 3.1.1.

   Labelling the zeros of $t^2 - 2$ as $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}$, the automorphisms ι and σ correspond to the identity (1) and the transposition (1 2).

2. For any $a, b, x, y \in \mathbb{R}$, $\phi(ax + by) = -(ax + by) = a(-x) + b(-y) = a\phi(x) + b\phi(y)$, so ϕ is a linear map of the real vector space $\mathbb{R}$.

   If $\phi(x) = \phi(y)$ then $-x = -y$, so $x = y$. Thus ϕ is injective.

   Every $x \in \mathbb{R}$ is $\phi(-x)$ where $-x \in \mathbb{R}$, so ϕ is surjective. Hence ϕ is bijective.

   However, $\phi(xy) = -xy$ but $\phi(x)\phi(y) = (-x)(-y) = xy$, so ϕ is not a field automorphism.

3. Let $x = a + b\mathrm{i}, y = c + d\mathrm{i}$ where $a, b, c, d \in \mathbb{R}$. Then $\sigma(x + y) = \sigma((a + c) + (b + d)\mathrm{i})$

   $= (a + c) - (b + d)\mathrm{i} = (a - b\mathrm{i}) + (c - d\mathrm{i}) = \sigma(x) + \sigma(y)$

   and $\sigma(xy) = \sigma((ac-bd)+(ad+bc)\mathrm{i}) = (ac-bd)-(ad+bc)\mathrm{i}$

   $= (a - b\mathrm{i})(c - d\mathrm{i}) = \sigma(x)\sigma(y)$. Thus σ is a homomorphism from $\mathbb{C}$ to $\mathbb{C}$.

If $\sigma(x) = 0$, i.e. $a - b\mathrm{i} = 0$, then $a = b = 0$, so $x = 0$. Thus $\operatorname{Ker}\sigma = \{0\}$, so σ is injective. Clearly σ is also surjective and thus it is bijective, i.e. σ is an automorphism of $\mathbb{C}$.

4. Any automorphism σ of $\mathbb{Q}(3^{1/5})$ must map $3^{1/5}$ to some zero of its minimal polynomial $t^5 - 3$, by Proposition 3.3.

   As $3^{1/5}$ is the only real zero, the others are not in $\mathbb{Q}(3^{1/5})$ so the only possible value of $\sigma(3^{1/5})$ is $3^{1/5}$.

   The effect of σ on $3^{1/5}$ determines its effect on $\mathbb{Q}(3^{1/5})$, so σ can only be the identity map.

5. By Proposition 3.3, any automorphism σ of $\mathbb{Q}(\varepsilon)$ maps ε to some zero of its minimal polynomial, which is the cyclotomic polynomial Φ_p.

   The zeros of Φ_p are ε^k for $k = 1, \ldots, p-1$, so $\sigma(\varepsilon)$ must be one of these.

Exercises 3.2

1. By considering the splitting fields, and using Proposition 3.9 in the irreducible cases, the Galois groups are isomorphic to:

   (a) S_3, (b) S_2, (c) $\{\iota\}$. (d) S_3, (e) A_3.

   Note that in (b) the splitting field is $\mathbb{Q}(\omega)$. The Galois group is that of the irreducible quadratic factor $t^2 + t + 1$.

   In (c) the splitting field is $\mathbb{Q}$, and the only $\mathbb{Q}$-automorphism of $\mathbb{Q}$ is the identity.

2. (a) We find $\mu = t^4 - 10t^2 + 20$, which has zeros are $\pm\sqrt{5 \pm \sqrt{5}}$, i.e. $\pm\alpha, \pm\beta$.

$\alpha\beta = \sqrt{20} = 2\sqrt{5} = 2(\alpha^2 - 5)$ so $\beta = \dfrac{2(\alpha^2-5)}{\alpha}$. This is obtained by field operations on elements of $\mathbb{Q}$ and α, so it is in $\mathbb{Q}(\alpha)$.

Then $-\alpha, -\beta \in \mathbb{Q}(\alpha)$, so the splitting field of μ is contained in $\mathbb{Q}(\alpha)$.

No proper subfield of $\mathbb{Q}(\alpha)$ contains α, so $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial\mu = 4$.

(b) The Galois group $\Gamma(\mathbb{Q}(\alpha) : \mathbb{Q})$ is transitive on the set of zeros of f, so there is an element σ which maps α to β.

$\sigma(\alpha)\sigma(\beta) = \sigma(\alpha\beta) = \sigma(2(\alpha^2 - 5)) = 2(\sigma(\alpha)^2 - 5) = 2(\beta^2 - 5) = -2\sqrt{5} = -\alpha\beta$, so $\sigma(\beta) = \dfrac{-\alpha\beta}{\sigma(\alpha)} = \dfrac{-\alpha\beta}{\beta} = -\alpha$.

Thus $\sigma^2(\alpha) = \sigma(\beta) = -\alpha,\ \sigma^3(\alpha) = \sigma(-\alpha) = -\beta,$ $\sigma^4(\alpha) = \sigma(-\beta) = \alpha$.

(c) Since $\mathbb{Q}(\alpha)$ is a normal, finite extension it is a Galois extension, so the Galois group has order 4. We have found four automorphisms, so there are no more.

$\Gamma(\mathbb{Q}(\alpha) : \mathbb{Q}) = \{\iota, \sigma, \sigma^2, \sigma^3\}$ where $\sigma^4 = \iota$, so the Galois group is cyclic, isomorphic to C_4.

3. (a) $\alpha\beta = 1$ so $\beta \in \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$. By Proposition 3.2, $\sigma(\alpha)$ determines the effect of σ on $\mathbb{Q}(\alpha)$.

$\mathbb{Q}(\alpha) : \mathbb{Q}$ is a Galois extension, so $\Gamma_{\mathbb{Q}}(\mathrm{f}) = \Gamma(\mathbb{Q}(\alpha) : \mathbb{Q})$ has order 4.

Let $\sigma(\alpha) = \beta$; there is such an automorphism by Proposition 3.6.

Then $\sigma(\alpha)\sigma(\beta) = \sigma(\alpha\beta) = \sigma(1) = 1$,

so $\sigma(\beta) = \dfrac{1}{\sigma(\alpha)} = \dfrac{1}{\beta} = \alpha$.

Let $\tau(\alpha) = -\alpha$; there is such an automorphism by Proposition 3.6. Then $\sigma\tau(\alpha) = -\beta$.

We have found automorphisms which map α to each of its conjugates. Each is self-inverse, so $\Gamma_{\mathbb{Q}}(\mathrm{f}) = \{\iota, \sigma, \tau, \sigma\tau\}$ which is isomorphic to the Klein 4-group V.

4. (a) $\sigma(\gamma)$ is a conjugate of γ, i.e. a zero of f, so $\sigma(\gamma)$ can be $\gamma, -\gamma, \delta$ or $-\delta$.

$\sigma(\mathrm{i})$ must be a zero of $t^2 + 1$ (the minimal polynomial of i over $\mathbb{Q}$), i.e. i or $-\mathrm{i}$.

$\{1, \gamma, \gamma^2, \gamma^3, \mathrm{i}, \gamma\mathrm{i}, \gamma^2\mathrm{i}, \gamma^3\mathrm{i}\}$ is a basis for $\mathbb{Q}(\gamma, \mathrm{i})$ over $\mathbb{Q}$. The effect of σ on γ and i determines its effect on each basis element, hence on all of $\mathbb{Q}(\gamma, \mathrm{i})$.

(b) $\mathbb{Q}(\gamma, \mathrm{i}) : \mathbb{Q}$ is a Galois extension, so by Proposition 3.7 $\Gamma_{\mathbb{Q}}(\mathrm{f})$ has order 8. We have found 8 automorphisms (2 values of $\sigma(\mathrm{i})$ for each of 4 values of $\sigma(\gamma)$), so these must be all the elements of the Galois group, which is isomorphic to D_4 - see Examples 3.2.2. (i).

Exercises 3.3

1. (a) The zeros of f are the three cube roots of -2, i.e. they are $-\varepsilon, -\varepsilon\omega, -\varepsilon\omega^2$.

(b) As $\delta(\mathrm{f}) \notin \mathbb{Q}$, the Galois group is isomorphic to S_3.

The zeros of f are $-\varepsilon$, $\varepsilon\omega$, $\varepsilon\omega^2$ so the splitting field of f is $\mathbb{Q}(\varepsilon, \omega)$.

If $\sigma \in G$ then $\sigma(\varepsilon)$ is a zero of $t^3 - 2$ (the minimal polynomial of ε) and $\sigma(\omega)$ is a zero of $t^2 + t + 1$ (the minimal polynomial of ω). Hence the six $\mathbb{Q}$-automorphisms in G are:

$\iota : \varepsilon \mapsto \varepsilon, \omega \mapsto \omega, \qquad \sigma : \varepsilon \mapsto \varepsilon\omega, \omega \mapsto \omega, \qquad \sigma^2 : \varepsilon \mapsto \varepsilon\omega^2, \omega \mapsto \omega,$

$\tau : \varepsilon \mapsto \varepsilon, \omega \mapsto \omega^2, \quad \sigma\tau : \varepsilon \mapsto \varepsilon\omega, \omega \mapsto \omega^2, \quad \sigma^2\tau : \varepsilon \mapsto \varepsilon\omega^2, \omega \mapsto \omega^2.$

(c) Subgroup and subfield lattice structures as for Example 3.3.1. The only normal extension of $\mathbb{Q}$ is $\mathbb{Q}(\omega)$, corresponding to the normal subgroup A_3.

(d) Notice that $t^3 + 3t^2 + 3t + 3 = (t+1)^3 + 2$, so if x is a zero of $t^3 + 3t^2 + 3t + 3$ then $x + 1$ is a zero of f.

Thus the zeros are $-\varepsilon - 1, -\varepsilon\omega - 1, -\varepsilon\omega^2 - 1$, the splitting field is $\mathbb{Q}(\varepsilon, \omega)$ and the Galois group is S_3 as in (b).

2. It is straightforward to show that $\mathrm{f} = t^4 + 1$ is irreducible over $\mathbb{Q}$, e.g. by showing that it has no rational zeros and no quadratic factors in $\mathbb{Q}[t]$.

The zeros of f are the 4th roots of -1, which are $\pm\mathrm{e}^{\pi\mathrm{i}/4}$ $\pm\mathrm{e}^{3\pi\mathrm{i}/4}$ (or equivalent). Thus the splitting field of f is $\mathbb{Q}(\mathrm{e}^{\pi\mathrm{i}/4})$, which has degree 4 over $\mathbb{Q}$.

Let $\alpha = \mathrm{e}^{\pi\mathrm{i}/4}$. There are four automorphisms of $\mathbb{Q}(\alpha)$. They can be defined by their effect on α, which must be mapped to a zero of f:

$\iota : \alpha \mapsto \alpha,\ \sigma : \alpha \mapsto -\alpha,\ \tau : \alpha \mapsto \alpha^3,\ \sigma\tau : \alpha \mapsto -\alpha^3.$

These form a group G isomorphic to the Klein 4-group V.

The proper subgroups of G are $\{\iota, \sigma\}$, $\{\iota, \tau\}$, $\{\iota, \sigma\tau\}$. These respectively correspond to the fields $\mathbb{Q}(\alpha^2)$, $\mathbb{Q}(\alpha + \alpha^3)$, $\mathbb{Q}(\alpha - \alpha^3)$, or equivalently $\mathbb{Q}(\mathrm{i}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\mathrm{i}\sqrt{2})$. All the subgroups are normal in G and all the subfields are normal extensions of $\mathbb{Q}$, being the splitting fields of t^2+1, t^2-2, t^2+2 respectively. The lattices as in Example 3.3.2.

3. (a) If $u = t^2$, f $= u^2 - 30u + 25$, whose zeros for u are $\frac{1}{2}(30 \pm \sqrt{800}) = 15 \pm 10\sqrt{2}$.
Now $\alpha^2 = 5(3 + 2\sqrt{2}) = 15 + 10\sqrt{2}$, so α is a zero of f.
The other zeros of f are $-\alpha = -\sqrt{5}(\sqrt{2}+1), \sqrt{5}(\sqrt{2}-1), -\sqrt{5}(\sqrt{2}-1)$.

(b) $\alpha\sqrt{5}(\sqrt{2}-1) = 5(\sqrt{2}-1)(\sqrt{2}+1) = 5$.
$\alpha - \dfrac{5}{\alpha} = 2\sqrt{5}$ so $\sqrt{5} = \dfrac{1}{2}\left(\alpha - \dfrac{5}{\alpha}\right)$ is in $\mathbb{Q}(\alpha)$. Then
$\sqrt{2} = \dfrac{\sqrt{5}}{\alpha} + 1 \in \mathbb{Q}(\alpha)$, so $\mathbb{Q}(\sqrt{5}, \sqrt{2}) \subset \mathbb{Q}(\alpha)$.
Clearly $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{5}, \sqrt{2})$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5}, \sqrt{2})$,
All the zeros of f are in $\mathbb{Q}(\sqrt{5}, \sqrt{2})$, and the splitting field of f must contain $\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5}, \sqrt{2})$ is the splitting field of f over $\mathbb{Q}$.

(c) The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$, so a basis for M over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$. $[M : \mathbb{Q}] = 2$.
The minimal polynomial of $\sqrt{5}$ over M is $t^2 - 5$, so a basis for L over M is $\{1, \sqrt{5}\}$. $[L : M] = 2$.
By the Tower law, a basis for L over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ and so $[L : \mathbb{Q}] = 4$.

(d) $(t^2 - 2)(t^2 - 5) = t^4 - 7t^2 + 10$ also has splitting field $\mathbb{Q}(\sqrt{5}, \sqrt{2})$.

(e) Yes. By the methods shown in Chapter 2 we can construct $\sqrt{5}$ and $\sqrt{2}$, then $\sqrt{2} + 1$, then the product $\sqrt{5}(\sqrt{2} + 1)$.

(f) $L : \mathbb{Q}$ is a Galois extension, as L is the splitting field of f over $\mathbb{Q}$. Hence $|G| = [L : \mathbb{Q}]$.

(g) $|G| = 4$. Up to isomorphism the only groups of order 4 are C_4 and V so, as G is not cyclic, $G \cong V$.

The elements of G are
$\iota : \sqrt{2} \mapsto \sqrt{2}, \sqrt{5} \mapsto \sqrt{5},\ \sigma : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{5} \mapsto \sqrt{5},$
$\tau : \sqrt{2} \mapsto \sqrt{2}, \sqrt{5} \mapsto -\sqrt{5},\ \sigma\tau : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{5} \mapsto$
$-\sqrt{5}$.

(h) Lattices as in Example 3.3.2.

There are three intermediate fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{10})$, both normal extensions of $\mathbb{Q}$ as they are the splitting fields of $t^2 - 2, t^2 - 5, t^2 - 10$.

These are respectively the fixed fields of three normal subgroups of G, all isomorphic to S_2, namely $\{\iota, \tau\}$, $\{\iota, \sigma\}$, $\{\iota, \sigma\tau\}$.

4. (a) If $x^2 - 4x + 6 = 0,\ x = \frac{1}{2}(4 \pm \sqrt{-8}) = 2 \pm \sqrt{-2}$.

Hence the four zeros of f are $\pm\sqrt{2 \pm \mathrm{i}\sqrt{2}}$.

(b) $\alpha\beta = (\sqrt{2 + \mathrm{i}\sqrt{2}})(\sqrt{2 - \mathrm{i}\sqrt{2}}) = \sqrt{(2 + \mathrm{i}\sqrt{2})(2 - \mathrm{i}\sqrt{2})} =$

$\sqrt{6}$. $\quad \beta = \dfrac{\sqrt{6}}{\alpha} \in L = \mathbb{Q}(\alpha, \sqrt{6})$.

Also $-\alpha, -\beta \in L$ so all the zeros of f are in L, hence the splitting field of f is contained in L.

No proper subfield of L can contain both α and β, so L is the splitting field of f over $\mathbb{Q}$.

(c) Min. poly. of α over $\mathbb{Q}$ is f, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Min. poly. of $\sqrt{6}$ over $\mathbb{Q}(\alpha)$ is $t^2 - 6$, so $[L : \mathbb{Q}(\alpha)] = 2$. Thus by the Tower Law, $[L : \mathbb{Q}] = 8$.

(d) We must have $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$, so $\sigma(\sqrt{6}) = \beta\sigma(\beta)$.

Thus $\sigma(\beta) = -\dfrac{\sqrt{6}}{\beta} = -\alpha$. $\quad \sigma^2(\alpha) = \sigma(\beta) = -\alpha$,

$\sigma^2(\sqrt{6}) = \sqrt{6}$,
$\sigma^3(\alpha) = \sigma(-\alpha) = -\beta,\ \sigma^3(\sqrt{6}) = -\sqrt{6}$,
$\sigma^4(\alpha) = \sigma(-\beta) = \alpha,\ \sigma^4(\sqrt{6}) = \sqrt{6}$.

(e) $\sigma^4 = \iota$ so $\{\iota, \sigma, \sigma^2, \sigma^3\} \cong C_4$, so it is a cyclic subgroup of the Galois group. $\Gamma_{\mathbb{Q}}(\mathrm{f})$ has order 8 so it is isomorphic to D_4.

(f) $H = \Gamma(L : M)$ is a normal subgroup of $G = \Gamma(L : \mathbb{Q})$. $G/H \cong \Gamma(M : \mathbb{Q})$.

5. The zeros of $\mathrm{f} = t^4 + t^3 + t^2 + t + 1$ are the complex fifth roots of unity, $\mathrm{e}^{2\pi \mathrm{i} k/5}$ for $k = 1, 2, 3, 4$. As these are all powers of $\eta = \mathrm{e}^{2\pi \mathrm{i}/5}$, the splitting field of f is $\mathbb{Q}(\eta)$, which has degree 4 over $\mathbb{Q}$.

   Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\eta)$ is determined by its effect on η, and must map η to a zero of $t^4 + t^3 + t^2 + t + 1$, i.e. one of $\eta, \eta^2, \eta^3, \eta^4$.

   Let $\sigma : \eta \mapsto \eta^2$. Then $\sigma^2 : \eta \mapsto \eta^4$, $\sigma^3 : \eta \mapsto \eta^8 = \eta^3$ and $\sigma^4 : \eta \mapsto \eta^{16} = \eta$.

   σ generates all possible $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\eta)$, so the Galois group G is cyclic of order 4, i.e. it is C_4.

   The only proper subgroup of G is $\{\iota, \sigma^2\}$. This corresponds to the subfield $\mathbb{Q}(\eta + \eta^4)$, i.e. $\mathbb{Q}(\cos(2\pi/5))$ or equivalently $\mathbb{Q}(\sqrt{5})$.

   The subgroup is normal in G and the subfield is a normal extension of $\mathbb{Q}$, being the splitting field of e.g. $t^2 + t - 1$ or $t^2 - 5$.

6. The splitting field of $\mathrm{f} = t^5 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \varepsilon)$ where $\alpha = 2^{1/5}$, $\varepsilon = \mathrm{e}^{2\pi \mathrm{i}/5}$.

   $[\mathbb{Q}(\alpha, \varepsilon) : \mathbb{Q}] = 20$, so $|\Gamma_{\mathbb{Q}}(\mathrm{f})| = 20$.

   The elements of the Galois group can be defined by their effect on α and ε, since this determines their effect on a basis for $\mathbb{Q}(\alpha, \varepsilon)$ over $\mathbb{Q}$.

Any automorphism must map each of α and ε to a zero of its minimal polynomial. There are five possibilities for the image of α and four for the image of ε, giving the required 20, so all possibilities will occur.

Let σ and τ be the automorphisms defined by

$\sigma(\alpha) = \alpha,\ \sigma(\varepsilon) = \varepsilon^2, \qquad \tau(\alpha) = \alpha\varepsilon,\ \tau(\varepsilon) = \varepsilon.$

Then $\sigma^2(\varepsilon) = \varepsilon^4,\ \sigma^2(\alpha) = \alpha,$

$\sigma^3(\varepsilon) = \varepsilon^3,\ \sigma^3(\alpha) = \alpha, \qquad \sigma^4(\varepsilon) = \varepsilon,\ \sigma^4(\alpha) = \alpha.$

Hence $\sigma^4 = \iota$, so σ generates a cyclic subgroup of order 4.

$\tau^2(\varepsilon) = \varepsilon,\ \tau^2(\alpha) = \alpha\varepsilon^2, \qquad \tau^3(\varepsilon) = \varepsilon,\ \tau^3(\alpha) = \alpha\varepsilon^3,$

$\tau^4(\varepsilon) = \varepsilon,\ \tau^4(\alpha) = \alpha\varepsilon^4, \qquad \tau^5(\varepsilon) = \varepsilon,\ \tau^5(\alpha) = \alpha\varepsilon^5 = \alpha.$

Hence $\tau^5 = \iota$, so τ generates a cyclic subgroup of order 5.

From a list of groups, e.g.
http://www.math.niu.edu/~beachy/courses/algebra/pedersen/small_groups.html

we find that $\Gamma_{\mathbb{Q}}(\mathrm{f}) \cong F_5$, the Frobenius group of order 20.

$\mathrm{Fix}(\langle\sigma\rangle) = \mathbb{Q}(\alpha), \quad \mathrm{Fix}(\langle\tau\rangle) = \mathbb{Q}(\varepsilon).$

$\mathbb{Q}(\alpha) : \mathbb{Q}$ is not a normal extension of $\mathbb{Q}$, as one but not all zeros of $t^5 - 2$ are in $\mathbb{Q}(\alpha)$.

$\mathbb{Q}(\varepsilon) : \mathbb{Q}$ is normal extension, as $\mathbb{Q}(\varepsilon)$ is the splitting field of $t^4 + t^3 + t^2 + t + 1$ over $\mathbb{Q}$.

Hence $\langle\sigma\rangle$ (the C_4 subgroup) is a normal subgroup of $\Gamma_{\mathbb{Q}}(\mathrm{f})$, but $\langle\tau\rangle$ (the C_5 subgroup) is not a normal subgroup of $\Gamma_{\mathbb{Q}}(\mathrm{f})$.

Other subgroups (e.g. $\{\iota, \sigma^2\}$) and corresponding subfields can be found with time and patience.

Exercises 3.4

1. Following the method in the proof of Proposition 3.17 with $\ell = 1$ and $m = 4$,

   $(2 \quad 5 \quad 3) = (4 \quad 5 \quad 2)^{-1}(1 \quad 3 \quad 2)^{-1}(4 \quad 5 \quad 2)(1 \quad 3 \quad 2)$.

2. Labelling the vertices $1, \ldots, n$ in sequence around the perimeter, the n-cycle $(1 \;\; 2 \;\; \cdots \;\; n)$ represents a rotation through $\dfrac{2\pi}{n}$ about the center of an n-gon, so it is a symmetry of the n-gon and is thus in D_n.

   Suppose p is a prime greater than 3. D_p contains the n-cycle $(1 \;\; 2 \;\; \cdots \;\; p)$ and all powers of it, so D_p is transitive on $\{1, \ldots, p\}$. If it also contained a transposition then by Proposition 3.18 it would be the whole of S_p, but $|D_p| = 2p \neq p! = |S_p|$. Hence there can be no transpositions in D_p.

   Geometrically, a transposition would swap just two vertices of a regular p-gon, but for $p \geq 3$ there is no symmetry which does this.

3. C_n is an abelian, hence solvable, group so a polynomial with Galois group C_n is solvable by radicals.

   $\{\iota\} \lhd C_n \lhd D_n$. C_n is solvable, and D_n/C_n is solvable as it has order 2, so D_n is solvable and thus a polynomial with Galois group D_n is solvable by radicals.

   A_n is not solvable for $n \geq 5$, since if it were then we would have a sequence $\{\iota\} \lhd G_1 \lhd \cdots \lhd A_n \lhd S_n$ with abelian quotients, but we know S_n is not solvable. Thus a polynomial with Galois group A_n is not solvable by radicals.

4. (a) $\mathrm{f} = t^5 - 10t + 2$ is irreducible over $\mathbb{Q}$ by EIC with $p = 2$.

   $\mathrm{Df} = 5t^4 - 10$ which has real zeros $\pm 2^{1/4}$.

The stationary points of f are at $(-2^{1/4}, 11.5)$ and $(2^{1/4}, -7.5)$. From a graph f has three real zeros; the other two are a complex conjugate pair.

Thus f has exactly two non-real zeros, so by Proposition 3.19 its Galois group is isomorphic to S_5. By Proposition 3.17 this is not a solvable group, so f is not solvable by radicals over $\mathbb{Q}$.

(b) $\mathrm{f} = t^7 - 7t^5 + 28t + 7$ is irreducible over $\mathbb{Q}$ by EIC with $p = 7$.

$\mathrm{Df} = 7t^6 - 35t^4 + 28 = 7(t+1)(t-1)(t^4 - 4t^2 - 4)$ which has real zeros $\pm 1, \pm\sqrt{2 + 2\sqrt{2}}$.

The stationary points of f are at $(-2.2, 56.7), (-1, -15), (1, 29), (2.2, -42.7)$. From a graph f has 5 real zeros; the others are a complex conjugate pair.

Thus f has exactly two non-real zeros, so by Proposition 3.19 its Galois group is isomorphic to S_7. By Proposition 3.17 this is not a solvable group, so f is not solvable by radicals over $\mathbb{Q}$.

5. Let f be the given polynomial. $\mathrm{f}(x) = 0$ iff x^2 is a zero of $at^4 + bt^3 + ct^2 + dt + e$. As this is quartic, it is solvable by radicals so its splitting field M is contained in a radical extension L of $\mathbb{Q}$.

   The zeros of f are square roots of elements of M, each of which lies in L or in a radical extension of L, which is in turn a radical extension of $\mathbb{Q}$.

   Hence the splitting field of f is contained in a radical extension of $\mathbb{Q}$, so f is solvable by radicals over $\mathbb{Q}$.

6. $\mathrm{f} = 4t^7 - 28t + 7$ is irreducible by EIC with $p = 7$. Its

degree is prime.

$\mathrm{Df} = 28t^6 - 28 = 28(t^6 - 1)$ which has real zeros ± 1.

The stationary points of f occur at $(-1, 31), (1, -17)$. By considering a graph, f has three real zeros. The other four are two complex conjugate pairs.

Thus f has neither just one real zero nor seven real zeros, so by the given fact it is not solvable by radicals over $\mathbb{Q}$.