MAT3011 GALOIS THEORY ANSWERS FOR CHAPTER 1

Exercises 1.1

1. (a) $(\mathbb{N}, +, \times)$ is not a ring, as there is no additive identity in $\mathbb{N} = \{1, 2, 3, \ldots\}$.

   (b) $(\mathbb{Z}_6, +_6, \times_6)$ is not an ID. $2 \times_6 3 = 0$, so 2 and 3 are zero-divisors.

   (c) $\mathbb{R}[t]$ is an integral domain, because $\mathbb{R}$ is a field and hence an ID.

   (d) $\mathbb{C}[t]$ is not a field. Polynomials over a field do not, in general, have multiplicative inverses that are polynomials. ($\mathbb{C}(t)$ *is* a field, however, consisting of quotients of polynomials over $\mathbb{C}$).

   (e) Let $\mathrm{f} = \mathrm{i}t^3 - 12\mathrm{i}t - \pi$, so $\mathrm{Df} = 3\mathrm{i}t^2 - 12\mathrm{i}$, which has zeros ± 2. Neither of these is a zero of f, so f has no repeated zeros. By the Fundamental Theorem of Algebra, f is a product of three linear factors over $\mathbb{C}$ so it has three distinct zeros in $\mathbb{C}$.

   (f) Yes; it's just a place holder. Many books use x for the indeterminate, but this can cause problems (over finite fields) if x is also used for a variable or unknown. It's best to use t.

   (g) No. A polynomial is just a formal sum of algebraic terms. It defines, but is not in itself, a function.

   (h) Yes. $\mathbb{Q}(t)$ consists of quotients of polynomials. Those with denominators in $\mathbb{Q}$ are in $\mathbb{Q}[t]$. The polynomials of degree 0 are in $\mathbb{Q}$.

   (i) No. $\mathbb{Z}_4$ is not a field; it is not even an integral domain, since 2 is a zero-divisor. Recall that in Groups & Rings, $\mathbb{F}_4$ was constructed by adjoining the zeros of $t^2 + t + 1$ to $\mathbb{F}_2$.

(j) Yes. f(0) = 1, f(1) = 1, so f has no zeros in $\mathbb{F}_2 = \{0, 1\}$ $\mathbb{F}_4$ is constructed precisely so that it contains the zeros of t^2+t+1. (Technically it is $\mathbb{F}_2/\langle \mathrm{f} \rangle$, in which $\mathrm{f}(t+\langle \mathrm{f} \rangle) = \langle \mathrm{f} \rangle$, the zero coset. Letting $\alpha = t+\langle \mathrm{f} \rangle$, the zeros of f are α and $1+\alpha$. We won't need the formal construction in this module, just the fact that there *is* a field containing the zeros.)

(k) No. $\mathbb{F}_2$ is a subfield (in fact the prime subfield) of $\mathbb{F}_4$, but $\mathbb{F}_2$ is NOT a subfield of $\mathbb{F}_3$ where the operations are different (mod 3, not mod 2).

(l) No. $\mathbb{F}_p(t)$ is an example of an infinite field of characteristic $p \neq 0$.

2. We find that 1 and 2 are zeros of f, so $t-1$ and $t-2$ are factors of f. By division or by inspection, $\mathrm{f} = (t-1)(t-2)(t^2-2) = (t-1)(t-2)(t-\sqrt{2})(t+\sqrt{2})$.
$\Delta(\mathrm{f}) = [(1-2)(1-\sqrt{2})(1+\sqrt{2})(2-\sqrt{2})(2+\sqrt{2})(\sqrt{2}+\sqrt{2})]^2 = 32$.

3. Let α be a zero of f, so $\mathrm{f} = (t-\alpha)\mathrm{h}$ for some polynomial h.

   Then by the product rule, $\mathrm{Df} = (t-\alpha)\mathrm{Dh} + \mathrm{h}$.

   If also α is a zero of Df then $(t-\alpha)$ is a factor of Df, so $(t-\alpha)\mathrm{Dh} + \mathrm{h} = (t-\alpha)\mathrm{k}$, say. Hence $\mathrm{h} = (t-\alpha)(\mathrm{k} - \mathrm{Dh})$.

   Then $\mathrm{f} = (t-\alpha)\mathrm{h} = (t-\alpha)^2(\mathrm{k} - \mathrm{Dh})$, so $(t-\alpha)^2$ is a factor of f.

   Thus α is a repeated zero of f. □

4. Let $\mathrm{f} = t^n + t + c$. If $n = 1$ then $\mathrm{f} = 2t + c$, which clearly has no repeated zeros.

Now assume $n > 1$. If f has a rational zero then, by the Rational Root theorem, this must be an integer which divides c.

Df $= nt^{n-1} + 1$. A repeated zero of f must also be a zero of Df.

Any rational zero of Df must have the form $\frac{p}{q}$ where $p \mid 1$, $q \mid n$, so the only integer possibilities are ± 1. But $\mathrm{Df}(1) = n+1 \neq 0$ and $\mathrm{Df}(-1) = \pm n + 1 \neq 0$, since $n > 1$.

Thus Df has no integer zeros, so f has no repeated rational zeros.

5. (a) Any rational zeros of $\mathrm{f} = 2t^3 + 5t^2 - 1$ have the form $\frac{p}{q}$ where $p \mid 1, q \mid 2$. Thus the possibilities are $\pm 1, \pm 1/2$. Now $\mathrm{f}(-1) = 2$, $\mathrm{f}(1) = 6$, $\mathrm{f}(1/2) = 1/2$, $\mathrm{f}(-1/2) = 0$ so the only rational zero of f is $-1/2$.

   (b) Any rational zeros of $\mathrm{f} = t^4 + 2t^3 - t - 2$ divide 2, so they can only be $\pm 1, \pm 2$. Now $\mathrm{f}(-2) = 0$, $\mathrm{f}(-1) = -2$, $\mathrm{f}(1) = 0$, $\mathrm{f}(2) = 28$, so the only rational zeros of f are -2 and 1.

   (c) Zeros of $\mathrm{f} = t^4 - 3t^2 + 2t - \frac{1}{3}$ are also zeros of $3\mathrm{f} = 3t^4 - 9t^2 + 6t - 1 \in \mathbb{Z}[t]$, so they have the form $\frac{p}{q}$ where $p \mid 1, q \mid 3$.

   Thus the possibilities are $\pm 1, \pm 1/3$. We find that $3\mathrm{f}(1) \neq 0$, $3\mathrm{f}(-1) \neq 0$, $3\mathrm{f}(1/3) \neq 0$, $3\mathrm{f}(-1/3) \neq 0$, so there are no rational zeros.

6. (a) Let f be the given polynomial. In $\mathbb{F}_5$ we have $\mathrm{f}(0) = 3$, $\mathrm{f}(1) = 2$, $\mathrm{f}(2) = 3$, $\mathrm{f}(3) = \mathrm{f}(-2) = 3$, $\mathrm{f}(4) = \mathrm{f}(-1) = 4$. Thus f has no zeros in $\mathbb{F}_5$.

   (b) Let g be the given polynomial. In $\mathbb{F}_5$ we have $\mathrm{g}(0) =$

3, g(1) = 0, g(2) = 4, g(3) = 2, g(4) = 1. Dg = $t^2 + 4$, so Dg(1) = 0. Thus 1 is a repeated zero of g.

7. In $\mathbb{F}_7$ we have f(0) = 3, f(1) = 4, f(2) = 5, f(3) = 2, f(4) = 0, f(5) = 0, f(6) = 0, so f has factors $t-4, t-5, t-6$, or equivalently $t+1, t+2, t+3$.

   Dividing successively by these (or dividing once by their product), modulo 7, we get f = $(t+1)(t+2)(t+3)(t^2+t+4)$.

8. (a) The required quadratic is $t^2 - 6t - 10$.

   (b) The required cubic is $t^3 + t^2 - t + 1$.

   (Do not write "= 0". You are just asked for the polynomials in t.)

9. $\alpha + \beta = -b = 5, \alpha\beta = c = -4$. Hence $\alpha^2 + \beta^2 = (\alpha+\beta)^2 - 2\alpha\beta = (-5)^2 - 2(-4) = 33$ and $\alpha^2\beta^2 = (\alpha\beta)^2 = (-4)^2 = 16$

   The quadratic with zeros α^2 and β^2 is thus $t^2 - 33t + 16$.

10. $(\alpha + \beta + \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2\alpha\beta + 2\alpha\gamma + 2\beta\gamma$ (as you should know).

    $s_1(\alpha, \beta, \gamma) = \alpha + \beta + \gamma = -5$, $s_2(\alpha, \beta, \gamma) = \alpha\beta + \beta\gamma + \gamma\alpha = -10$,

    so $\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = {s_1}^2 - 2s_2 = 45$.

Exercises 1.2

Note that complex exponentials can be expressed in more than one way, since $e^{k\pi i/n} = e^{(2mn-k)\pi i/n}$ for any $m \in \mathbb{Z}$. Thus $e^{8\pi i/5} = e^{-2\pi i/5}$, etc. Some people take the principal value of the argument to be in $(-\pi, \pi]$, others in $[0, 2\pi)$. Either is acceptable here.

1. The primitive fifth roots of 1 are $e^{2\pi i/5}$, $e^{4\pi i/5}$, $e^{6\pi i/5}$, $e^{8\pi i/5}$.

   The primitive sixth roots of 1 are $e^{\pi i/3}$, $e^{5\pi i/3}$.

   The primitive tenth roots of 1 are $e^{\pi i/5}$, $e^{3\pi i/5}$, $e^{7\pi i/5}$, $e^{9\pi i/5}$.

   The primitive twelfth roots of 1 are $e^{\pi i/6}$, $e^{5\pi i/6}$, $e^{7\pi i/6}$, $e^{11\pi i/6}$.

2. (a) The zeros of $t^{10} - 1$ are the tenth roots of 1,
   so they are $e^{2k\pi i/10}$ for $k = 0, \ldots, 9$.

   (b) The zeros of $t^4 + 1$ are the fourth roots of -1.
   Now $-1 = e^{\pi i}$ so one fourth root of -1 is $e^{\pi i/4}$.
   The others are found by multiplying this by the fourth roots of 1, namely 1, i, -1, $-$i, to get $e^{\pi i/4}$, $e^{3\pi i/4}$, $e^{5\pi i/4}$, $e^{7\pi i/4}$, or equivalently $\pm\dfrac{\sqrt{2}}{2}(1 \pm i)$.

   (c) The zeros of $(t-2)^5 - 32$ are values of $x \in \mathbb{C}$ such that $(x-2)^5 = 32$.
   Now $32 = 2^5$ so the fifth roots of 32 are $2e^{2k\pi i/5}$ for $k = 0, \ldots, 4$.
   Thus the required zeros are 4, $2 + 2e^{2\pi i/5}$, $2 + 2e^{4\pi i/5}$, $2 + 2e^{6\pi i/5}$,
   $2 + 2e^{8\pi i/5}$, or equivalent expressions.

3. (a) The zeros of $t^3 - 16$ are the three cube roots of 16, which are $2\varepsilon, 2\varepsilon\omega, 2\varepsilon\omega^2$ where $\varepsilon = 2^{1/3}$ and $\omega = e^{2\pi i/3}$.
   $\Delta(f) = -27 \times (-16)^2 = -6912$.

   (b) The zeros of t^3+1 are the cube roots of -1, i.e. $-1, -\omega, -\omega^2$.
   $\Delta(f) = -27$.

   (c) $t^3 - 3t - 2 = (t+1)(t^2 - t - 2) = (t+1)(t+1)(t-2)$
   so the zeros are $-1, -1, 2$. $\quad \Delta(f) = 0$.

   (d) To solve $x^3 + 6x + 2 = 0$ let $x = z - \dfrac{2}{z}$, giving

$z^3 - 6z + \dfrac{12}{z} - \dfrac{8}{z^3} + 6z - \dfrac{12}{z} + 2.$

Multiply through by z^3 to get $z^6 + 2z^3 - 8 = 0$, so $(z^3 - 2)(z^3 + 4) = 0$.

Thus $z^3 = 2$ or $z^3 = -4$.

Take $z^3 = 2$, so $z = \varepsilon, \varepsilon\omega, \varepsilon\omega^2$ where $\varepsilon = 2^{1/3}$, $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$.

Now $\dfrac{2}{\varepsilon} = \varepsilon^2$ and $\dfrac{1}{\omega} = \omega^2$ (since $\varepsilon^3 = 2$ and $\omega^3 = 1$).

Thus the zeros are $\varepsilon(1 - \varepsilon)$, $\varepsilon\omega(1 - \varepsilon\omega)$, $\varepsilon\omega(\omega - \varepsilon)$.

$\Delta(\mathrm{f}) = -972$.

(e) To solve $x^3 - 9x - 9 = 0$ let $x = z + \dfrac{3}{z}$, so $z^6 - 9z^3 + 27 = 0$.

$$z^3 = \frac{9 \pm 3\sqrt{3}\mathrm{i}}{2} = 3\sqrt{3}\left(\frac{\sqrt{3}}{2} \pm \frac{1}{2}\mathrm{i}\right) = 3\sqrt{3}\mathrm{e}^{\pm\mathrm{i}\pi/6},$$

so one value of z is $z_1 = (3\sqrt{3}\mathrm{e}^{\mathrm{i}\pi/6})^{1/3} = \sqrt{3}\mathrm{e}^{\pi\mathrm{i}/18}$.

The other values of z are $z_1\omega, z_1\omega^2$.

Thus $x = \sqrt{3}(\mathrm{e}^{\pi\mathrm{i}/18} + \mathrm{e}^{-\pi\mathrm{i}/18})$, $\sqrt{3}(\mathrm{e}^{11\pi\mathrm{i}/18} + \mathrm{e}^{-11\pi\mathrm{i}/18})$, $\sqrt{3}(\mathrm{e}^{13\pi\mathrm{i}/18} + \mathrm{e}^{-13\pi\mathrm{i}/18})$

$$= 2\sqrt{3}\cos\frac{\pi}{18},\ 2\sqrt{3}\cos\frac{11\pi}{18},\ 2\sqrt{3}\cos\frac{13\pi}{18}.$$

Alternatively let $x = r\cos\theta$, so we must find r, θ such that

$r^3\cos^3\theta - 9r\cos\theta - 9 = 0$.

Thus $\dfrac{r^3}{4}\cos 3\theta + \dfrac{3r^3}{4}\cos\theta - 9r\cos\theta - 9 = 0$.

Solve $\dfrac{3r^3}{4} - 9r = 0$ and $\dfrac{r^3}{4}\cos 3\theta - 9 = 0$.

Thus $r^3 = 12r$. Take $r = 2\sqrt{3}$, so $\cos 3\theta = \dfrac{\sqrt{3}}{2}$.

$3\theta = \dfrac{\pi}{6}, \dfrac{11\pi}{6}, \dfrac{13\pi}{6}$.

Then the zeros are the values of $r\cos\theta$, i.e.
$2\sqrt{3}\cos\frac{\pi}{18},\ 2\sqrt{3}\cos\frac{11\pi}{18},\ 2\sqrt{3}\cos\frac{13\pi}{18}$, as before. ($\approx 3.41, -2.23, -1.18$).
$\Delta(\mathrm{f}) = -4(-729) - 27(81) = 729.$

4. (a) By Proposition 1.3, $\alpha+\beta+\gamma = 0$ and $\alpha\beta\gamma = -q$, so $\beta+\gamma = -\alpha,\ \beta\gamma = -\frac{q}{\alpha}$.
α is a zero of f so $\alpha^3 + p\alpha + q = 0$. Thus $\alpha^2 + p = -\frac{q}{\alpha}$, so $\beta\gamma = \alpha^2 + p$.

   (b) $\mathrm{f} = (t-\alpha)(t-\beta)(t-\gamma) = (t-\alpha)(t^2+\alpha t+\alpha^2+p)$, so β, γ are the zeros of $t^2+\alpha t+(\alpha^2+p)$, which by the quadratic formula are $\frac{-\alpha \pm \sqrt{-3\alpha^2-4p}}{2}$.

   (c) $\delta(\mathrm{f}) = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$
$= \left(\frac{3\alpha - \sqrt{-3\alpha^2-4p}}{2}\right)\left(\frac{3\alpha+\sqrt{-3\alpha^2-4p}}{2}\right)\sqrt{-3\alpha^2-4p}$
$= \frac{1}{4}(9\alpha^2 - (-3\alpha^2-4p))\sqrt{-3\alpha^2-4p} = (3\alpha^2+p)\sqrt{-3\alpha^2-4p}$,
so $\Delta(\mathrm{f}) = \delta(\mathrm{f})^2 = (3\alpha^2+p)^2(-3\alpha^2-4p) = -(3\alpha^2+4p)(3\alpha^2+p)^2$.
$\delta(\mathrm{f}) = \sqrt{-3\alpha^2-4p}(3\alpha^2+p)$ so if $\delta(\mathrm{f}) \in \mathbb{Q}$ then $\sqrt{-3\alpha^2-4p} = \frac{\delta(\mathrm{f})}{3\alpha^2+p}$ is a rational function of α. Hence by (b), so are β and γ.

   (d) Let α be the given zero $-2^{1/3}-2^{2/3}$,
so $\alpha^2 = 2^{2/3} + 2^{4/3} + 2(2^1) = 2^{2/3} + 2(2^{1/3}) + 4$.
Here $p = -6$, so by (b)
$\beta,\gamma = \frac{2^{1/3}+2^{2/3} \pm \sqrt{12 - 3(2^{2/3}) - 6(2^{1/3})}}{2}$
$= \frac{2^{1/3}+2^{2/3} \pm \sqrt{-3((2^{2/3}) + 2(2^{1/3}) - 4)}}{2}$

$$= \frac{2^{1/3} + 2^{2/3} \pm \mathrm{i}\sqrt{3}(2^{1/3} - 2^{2/3})}{2}.$$

5. $x^3+bx^2+cx+d = (y-b/3)^3+b(y-b/3)^2+c(y-b/3)+d$
$= y^3-by^2+b^2y/3-b^3/27+by^2-2b^2y/3+b^3/9+cy-bc/3+d$
$= y^3 + (c - b^2/3)y + (d - bc/3 + 2b^3/27)$,
so $p = c - \dfrac{b^2}{3}$, $q = d - \dfrac{bc}{3} + \dfrac{2b^3}{27}$.
Let $x^3 + bx^2 + cx + d = 0$ have roots $x = \alpha_1, \alpha_2, \alpha_3$. Then $y^3 + py + q = 0$ has roots $y = \alpha_1 + \dfrac{b}{3}, \alpha_2 + \dfrac{b}{3}, \alpha_3 + \dfrac{b}{3}$, so the discriminant of $y^3 + py + q$ is
$$\left((\alpha_1 + \frac{b}{3} - [\alpha_2 + \frac{b}{3}])(\alpha_1 + \frac{b}{3} - [\alpha_3 + \frac{b}{3}])(\alpha_2 + \frac{b}{3} - [\alpha_3 + \frac{b}{3}])\right)^2$$
$= [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)]^2$
= discriminant of $x^3 + bx^2 + cx + d$.

6. Let the two values of z^3 be ε^3 and ζ^3. Their product $\varepsilon^3\zeta^3$ is the constant term in the quadratic, $-\dfrac{p^3}{27}$, so $\varepsilon\zeta = -\dfrac{p}{3}$.
Hence $\zeta = -\dfrac{p}{3\varepsilon}$ and $\varepsilon = -\dfrac{p}{3\zeta}$.
Thus $\varepsilon - \dfrac{p}{3\varepsilon} = \zeta - \dfrac{p}{3\zeta}$, $\varepsilon\omega - \dfrac{p\omega^2}{3\varepsilon} = \zeta\omega^2 - \dfrac{p\omega}{3\zeta}$,
$\varepsilon\omega^2 - \dfrac{p\omega}{3\varepsilon} = \zeta\omega - \dfrac{p\omega^2}{3\zeta}$,
so using ε or ζ gives the same values of y, hence of x.

7. (a) $\begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix} \longrightarrow \begin{vmatrix} 1 & 0 & 0 \\ \alpha & \beta-\alpha & \gamma-\alpha \\ \alpha^2 & \beta^2-\alpha^2 & \gamma^2-\alpha^2 \end{vmatrix}$ $\begin{matrix} \\ C_2 := C_2 - C_1 \\ C_3 := C_3 - C_1 \end{matrix}$
$= (\beta - \alpha)(\gamma^2 - \alpha^2) - (\gamma - \alpha)(\beta^2 - \alpha^2)$ (expanding by Row 1)

$= (\beta-\alpha)(\gamma-\alpha)(\gamma+\alpha) - (\gamma-\alpha)(\beta-\alpha)(\beta+\alpha) = (\gamma-\alpha)(\beta-\alpha)[(\gamma+\alpha)-(\beta+\alpha)]$

$= (\gamma-\alpha)(\beta-\alpha)(\gamma-\beta) = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha).$

(b) α, β, γ are zeros of $\mathrm{f} = t^3 + pt + q$,

so $\alpha+\beta+\gamma = 0$, $\alpha\beta+\beta\gamma+\gamma\alpha = p$, $\alpha\beta\gamma = -q$.

Thus $\alpha^2+\beta^2+\gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\beta\gamma+\gamma\alpha) = -2p$.

$\mathrm{f}(\alpha) = \mathrm{f}(\beta) = \mathrm{f}(\gamma) = 0$ so $\alpha^3+p\alpha+q = 0$, $\beta^3+p\beta+q = 0$, $\gamma^3+p\gamma+q = 0$.

Adding, $\alpha^3+\beta^3+\gamma^3+p(\alpha+\beta+\gamma)+3q = 0$, so $\alpha^3+\beta^3+\gamma^3 = -3q$.

Also $\alpha^4+p\alpha^2+q\alpha = 0$, $\beta^4+p\beta^2+q\beta = 0$, $\gamma^4+p\gamma^2+q\gamma = 0$.

Adding, $\alpha^4+\beta^4+\gamma^4+p(\alpha^2+\beta^2+\gamma^2)+q(\alpha+\beta+\gamma) = 0$, so $\alpha^4+\beta^4+\gamma^4 = -p(-2p) = 2p^2$.

Hence $\Delta(\mathrm{f}) = \det(\mathrm{V})^2 = \det(\mathrm{V})\det(\mathrm{V}^t) = \det(\mathrm{V}\mathrm{V}^t) = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix}$

$= 3(-4p^3-9q^2) - 2p(-4p^2) = -4p^3 - 27q^2.$

8. We may assume without loss of generality that f is monic.

Let $\mathrm{f} = t^3 + bt^2 + ct + d \in \mathbb{Q}[t]$, so product of zeros $= -d = (p+q\mathrm{i})(p-q\mathrm{i})r$.

Thus $|p+q\mathrm{i}|^2 = p^2+q^2 = (p+q\mathrm{i})(p-q\mathrm{i}) = -\dfrac{d}{r}$.

As $d \in \mathbb{Q}$ and $r \notin \mathbb{Q}$, this is irrational.

9. (a) First divide by 4 to get the monic quartic $t^4 - t^2 - 4t + \dfrac{5}{4}$, whose cubic resolvent is $t^3 + 2t^2 - 4t + 16$.

This equals $(t+4)(t^2-2t+4)$ which has a negative real zero -4.

Take $k = 2$, so $l + m = 3, m - l = -2, lm = \dfrac{5}{4}$, giving $l = \dfrac{5}{2}, m = \dfrac{1}{2}$.

Thus $\mathrm{f} = 4\left(t^2 + 2t + \dfrac{5}{2}\right)\left(t^2 - 2t + \dfrac{1}{2}\right)$ which has zeros $1 \pm \dfrac{1}{2}\sqrt{2}, -1 \pm \dfrac{1}{2}\mathrm{i}\sqrt{6}$.

(b) First divide by 4 to get the monic quartic $t^4 + 2t + \dfrac{3}{4}$, whose cubic resolvent is $t^3 + 3t + 4$. This has a negative real zero -1.

Take $k = 1$, so $l + m = 1, m - l = 2, lm = -\dfrac{3}{4}$, giving $l = -\dfrac{1}{2}, m = \dfrac{3}{2}$.

Thus $\mathrm{f} = 4\left(t^2 + t - \dfrac{1}{2}\right)\left(t^2 - t + \dfrac{3}{2}\right)$ which has zeros $\dfrac{1}{2}(-1 \pm \sqrt{3}), \dfrac{1}{2}(1 \pm \mathrm{i}\sqrt{5})$.

10. Let the zeros of the quartic be $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, so its discriminant is $\delta(\mathrm{f})^2$ where
$\delta(\mathrm{f}) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4)$.

The cubic resolvent has zeros $u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), v = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), w = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$. Its discriminant is $\delta(\rho)^2$ where $\delta(\rho) = (u - v)(u - w)(v - w)$.

Expanding $\delta(\mathrm{f})$ and $\delta(\rho)$, for which it would be a good idea to use computer algebra, we see that the discriminants are equal.

Exercises 1.3

1. Over $\mathbb{F}_2$, the eight cubics are $t^3, t^3+1, t^3+t, t^3+t+1, t^3+t^2, t^3+t^2+t, t^3+t^2+1, t^3+t^2+t+1$. All have 0 or 1 as a zero except t^3+t+1 and t^3+t^2+1 which are irreducible.

   Over $\mathbb{F}_3$, the 18 quadratics are $t^2, t^2+1, t^2+2, t^2+t, t^2+2t, t^2+t+1, t^2+t+2, t^2+2t+1, t^2+2t+2, 2t^2, 2t^2+1, 2t^2+2, 2t^2+t, 2t^2+2t, 2t^2+t+1, 2t^2+t+2, 2t^2+2t+1, 2t^2+2t+2$.

   All have 0, 1 or 2 as a zero except $t^2+1, t^2+t+2, t^2+2t+2, 2t^2+2$,
   $2t^2+t+1, 2t^2+2t+1$ which are irreducible.

2. (a) Content $= 14$. $\quad 28t^2-98t+56 = 14(2t^2-7t+4)$.

   (b) Content $= \dfrac{3}{16}$. $\quad \dfrac{3}{8}t^3-\dfrac{15}{16}t^2+\dfrac{3}{2}t-\dfrac{9}{4}$

   $= \dfrac{3}{16}(2t^3-5t^2+8t-12)$.

3. (a) Let $\mathrm{f} = t^3-4t+1$. As f is monic, any rational zero of divides 1. $\mathrm{f}(1) = -2$, $\mathrm{f}(-1) = 4$, so by the rational root theorem neither 1 nor -1 is a zero. Hence f has no linear factor so, as it is cubic, f is irreducible over $\mathbb{Q}$.

   (b) Let $\mathrm{f} = t^4+t+1$. $\mathrm{f}(1)$ and $\mathrm{f}(-1)$ are non-zero, so f has no linear factor. If it has quadratic factors then, as there is no t^3 term, they must be of the form $(t^2+at+1)(t^2-at+1)$ or $(t^2+at-1)(t^2-at-1)$. But both give a zero t term, so f has no such factors. Hence f is irreducible over $\mathbb{Q}$.

   (c) Let $\mathrm{f} = t^4+t^2+1$. As in (b) there are no linear factors. If $\mathrm{f} = (t^2+at+1)(t^2-at+1)$ then comparing coefficients of t^2 gives $2-a^2 = 1$. This has a solution when $a = 1$, so f is reducible over $\mathbb{Q}$ as $(t^2+t+1)(t^2-t+1)$.

   (d) t^4+6t^2+4t+2 is irreducible by EIC with $p = 2$.

(e) $2t^5 - 12t^3 + 15t^2 + 6$ is irreducible by EIC with $p = 3$.

(f) Reducing f modulo 2 we get $\nu_2(\mathrm{f}) = t^3 + t^2 + 1 \in \mathbb{F}_2[t]$. Neither 0 nor 1 is a zero of this, so there is no linear factor and hence, as it is cubic, $\nu_2(\mathrm{f})$ is irreducible over $\mathbb{F}_2$. By the localisation principle, f is irreducible over $\mathbb{Q}$.

(g) $t^6 - 15t^4 + 25t^2 + 5$ is irreducible by EIC with $p = 5$, so by Proposition 1.13, $5t^6 + 25t^4 - 15t^2 + 1$ is irreducible over $\mathbb{Q}$.

4. $\mathrm{f}(t+1) = t^6 + 6t^5 + 15t^4 + 21t^3 + 18t^2 + 9t + 3$, which is irreducible over $\mathbb{Q}$ by EIC with $p = 3$. Hence by Proposition 1.14, f is irreducible over $\mathbb{Q}$.

   $\mathrm{f} = (t^3)^2 + t^3 + 1$. If $x^2 + x + 1 = 0$ then $x = \mathrm{e}^{2\pi\mathrm{i}/3}$ or $x = \mathrm{e}^{4\pi\mathrm{i}/3}$.

   The zeros of f are the cube roots of these, i.e. they are $\mathrm{e}^{2\pi\mathrm{i}/9}$, $\mathrm{e}^{4\pi\mathrm{i}/9}$, $\mathrm{e}^{8\pi\mathrm{i}/9}$, $\mathrm{e}^{10\pi\mathrm{i}/9}$, $\mathrm{e}^{14\pi\mathrm{i}/9}$, $\mathrm{e}^{16\pi\mathrm{i}/9}$. Equivalently, they are $\mathrm{e}^{\pm 2\pi\mathrm{i}/9}$, $\mathrm{e}^{\pm 4\pi\mathrm{i}/9}$, $\mathrm{e}^{\pm 8\pi\mathrm{i}/9}$.

5. As f has no rational zeros, it has no factors of degree 1 in $\mathbb{Q}[t]$. If f is a product of two quadratic factors over $\mathbb{Q}$ then, as f has no t^3 term, they must have the form $(t^2 + at + b)(t^2 - at + c)$ where $a, b, c \in \mathbb{Z}$ by Gauss's lemma. Then $a^2 = b + c, a(c - b) = r, bc = p$.

   As p is prime, $\{b, c\} = \{1, p\}$ or $\{-1, -p\}$ so $a^2 = \pm(p+1)$. $a^2 > 0$ so we must have $a^2 = p + 1$. But then $p = (a - 1)(a + 1)$.
   The only possibility is $a = 2, p = 3, \{b, c\} = \{1, 3\}$.

   But this gives $\mathrm{f} = (t^2 + 2t + 1)(t^2 - 2t + 3)$, so $\mathrm{f}(-1) = 0$, or $\mathrm{f} = (t^2 - 2t + 1)(t^2 + 2t + 3)$, so $\mathrm{f}(1) = 0$. In each case f has a rational zero.

Hence if f has no rational zeros, it is irreducible over $\mathbb{Q}$.

6. $\mathrm{f}(t+1) = (t+1)^p + p - 1 = t^p + \sum_{r=1}^{p-1} \binom{p}{r} t^r + p.$

   We have shown in the notes that p divides $\binom{p}{r}$ for $r = 1, \ldots, p-1$.

   Also $p \not| \ 1$ and $p^2 \not| \ p$, so by EIC, $\mathrm{f}(t+1)$ is irreducible over $\mathbb{Q}$. By Proposition 1.14, the same is true of f.

7. If $a \neq kb^2$ for any $k, b \in \mathbb{Z}$, then a must have a prime factor p such that p^2 is not a factor of a. EIC with this prime p shows that $t^n - a$ is irreducible over $\mathbb{Q}$.

   No; e.g. take $a = 8 = 2 \times 2^2$ and $n = 2$. Then $t^2 - 8$ is irreducible over $\mathbb{Q}$, since $\sqrt{8}$ is irrational.

8. $\Phi_1 = t-1, \ \Phi_2 = t+1, \ \Phi_3 = t^2+t+1, \ \Phi_4 = t^2+1, \ \Phi_5 = t^4+t^3+t^2+t+1,$

   $\Phi_6 = t^2-t+1, \ \Phi_7 = t^6+t^5+t^4+t^3+t^2+t+1, \ \Phi_8 = t^4+1.$

9. f = qg + r as given in the question, so if f = pg then pg = qg + r.

   Thus (p − q)g = r. As ∂r < ∂g we must have p − q = 0, so p = q, so p $\in K[t]$.

10. As f has no rational zeros it has no factor of degree 1, so if f is reducible over $\mathbb{Q}$ then f = gh where g and h are irreducible over $\mathbb{Q}$ and both have degree 2. We have ν_p(f) = ν_p(g)ν_p(h).

    As ν_p(f) has a zero $\alpha \in \mathbb{F}_p$, $\nu_p(\mathrm{f}) = (t-\alpha)\mathrm{k}$ where k $\in \mathbb{F}_p[t]$ by Question 9 and ∂k = 3. As f has no other zero in $\mathbb{F}_p$, k must be irreducible over $\mathbb{F}_p$.

But $\nu_p(\mathrm{g})\nu_p(\mathrm{h}) = (t-\alpha)\mathrm{k}$ so either $\nu_p(\mathrm{g})$ or $\nu_p(\mathrm{h})$ has a factor which divides k in $\mathbb{F}_p[t]$, contradicting the irreducibility of k. Hence f is irreducible over $\mathbb{Q}$.

$t^4 + 10t + 1$ has no rational zeros, as neither 1 nor -1 is a zero of it.

$\nu_3(t^4 + 10t + 1) = t^4 + t + 1 = (t + 2)(t^3 + t^2 + t + 2)$.

The second factor has no zeros in $\mathbb{F}_3$ so $t^4 + t + 1$ has one zero, of multiplicity 1, in $\mathbb{F}_3$. Hence by the above, $t^4+10t+1$ is irreducible over $\mathbb{Q}$.

Exercises 1.4

1. Let $x = a + b\sqrt{c}$. Then $(x - a)^2 = b^2c$, so $x^2 - 2ax + a^2 - b^2c = 0$, i.e. x is a zero of $t^2 - 2at + (a^2 - b^2c) \in \mathbb{Q}[t]$ and is thus algebraic over $\mathbb{Q}$.

2. (a) $(\sqrt{21})^2 - 21 = 0$. $t^2 - 21$ is irreducible by EIC with $p = 3$ (or 7) so the minimal polynomial is $t^2 - 21$.

   $\sqrt{21}$ is algebraic of degree 2 over $\mathbb{Q}$. Its conjugate is $-\sqrt{21}$.

   (b) Let $\alpha = 2^{1/3} + 1$. Then $(\alpha - 1)^3 = 2$, so $\alpha^3 - 3\alpha^2 + 3\alpha - 3 = 0$.

   $t^3 - 3t^2 + 3t - 3$ is irreducible over $\mathbb{Q}$ by EIC with $p = 3$ (or by the RRT) so it is the minimal polynomial of α over $\mathbb{Q}$.

   α is algebraic of degree 3 over $\mathbb{Q}$. Its conjugates are $2^{1/3}\omega + 1, 2^{1/3}\omega^2 + 1$.

   (c) Let $\alpha = 3^{1/3} + 3^{2/3}$, so $\alpha^2 = 3^{2/3} + 3(3^{1/3}) + 6$, $\alpha^3 = 9(3^{1/3} + 3^{2/3}) + 12$.

   Thus $\alpha^3 = 9\alpha + 12$. Take $\mu = t^3 - 9t - 12$. Then α is a zero of μ, which is irreducible over $\mathbb{Q}$ by EIC with $p = 3$

(or by the RRT), so μ is the minimal polynomial of α over $\mathbb{Q}$.

α is algebraic of degree 3 over $\mathbb{Q}$. Solving the cubic, we find that the conjugates are $3^{1/3}\omega + 3^{2/3}\omega^2, 3^{1/3}\omega^2 + 3^{2/3}\omega$.

(d) Let $\alpha = \sqrt{6+\sqrt{6}}$. Then $\alpha^2 - 6 = \sqrt{6}$, so $\alpha^4 - 12\alpha^2 + 30 = 0$.

$t^4 - 12t^2 + 30$ is irreducible over $\mathbb{Q}$ by EIC with $p = 2$ (or 3), so it is the minimal polynomial of α over $\mathbb{Q}$.

α is algebraic of degree 4 over $\mathbb{Q}$.

Conjugates are $-\sqrt{6+\sqrt{6}}, \sqrt{6-\sqrt{6}}, -\sqrt{6-\sqrt{6}}$.

(e) $\mathrm{e}^{2\pi\mathrm{i}/5}$ is a primitive fifth root of 1, so its minimal polynomial over $\mathbb{Q}$ is $\Phi_5 = t^4 + t^3 + t^2 + t + 1$.

α is algebraic of degree 4 over $\mathbb{Q}$. Its conjugates are $\mathrm{e}^{4\pi\mathrm{i}/5}$, $\mathrm{e}^{6\pi\mathrm{i}/5}$, $\mathrm{e}^{8\pi\mathrm{i}/5}$.

(f) Let $\alpha = \mathrm{e}^{\pi\mathrm{i}/4}$. Then $\alpha^4 = \mathrm{e}^{\pi\mathrm{i}} = -1$ so α is a zero of $t^4 + 1$. This has no zeros in $\mathbb{Q}$, so has no linear factors. We can also check that it has no quadratic factors, so $t^4 + 1$ is irreducible over $\mathbb{Q}$ and hence is the minimal polynomial of α over $\mathbb{Q}$.

α is algebraic of degree 4 over $\mathbb{Q}$. Its conjugates are $\mathrm{e}^{3\pi\mathrm{i}/4}$, $\mathrm{e}^{5\pi\mathrm{i}/4}$, $\mathrm{e}^{7\pi\mathrm{i}/4}$.

3. Let $\alpha = \sqrt{p - \sqrt{p}}$. Then $(\alpha^2 - p)^2 = p$, so $\alpha^4 - 2p\alpha^2 + (p^2 - p) = 0$.

   p^2 cannot divide $p(p-1)$, so $t^4 - 2pt^2 + (p^2 - p)$ is irreducible over $\mathbb{Q}$ by EIC with the prime p and hence is the minimal polynomial of α over $\mathbb{Q}$.

4. $\alpha^3 = 1 + \mathrm{i}$, so $(\alpha^3 - 1)^2 = -1$. Thus $\alpha^6 - 2\alpha^3 + 2 = 0$.

   $t^6 - 2t^3 + 2$ is irreducible over $\mathbb{Q}$ by EIC with $p = 2$, so it is the minimal polynomial of α over $\mathbb{Q}$.

$\alpha \in \mathbb{C}$, so the minimal polynomial of α over $\mathbb{C}$ is $t - \alpha$.

5. $(z-a)^2 = -b^2$, so $z^2 - 2az + a^2 + b^2 = 0$.

   Hence z is a zero of $t^2 - 2at + (a^2 + b^2) \in \mathbb{R}[t]$. This cannot be reducible over $\mathbb{R}$, as its zeros are $a \pm b\mathrm{i} \notin \mathbb{R}$, so it is the minimal polynomial of α over $\mathbb{R}$.

6. Let $\alpha = 2^{1/4}\mathrm{i}$, so $\alpha^2 = -\sqrt{2}$, $\alpha^4 = 2$. The required minimal polynomials are:

   (a) $t^4 - 2$, (b) $t^2 + \sqrt{2}$, (c) $t^2 + \sqrt{2}$, (d) $t - 2^{1/4}\mathrm{i}$.

   The minimal polynomial is defined only over a *field*, so there is no such thing as the minimal polynomial over $\mathbb{Z}$.

7. Solving $\mu(x) = 0$ gives $x^2 = m + n \pm 2\sqrt{mn}$.

   Now $(\sqrt{m} + \sqrt{n})^2 = m + n + 2\sqrt{mn}$ and $(\sqrt{m} - \sqrt{n})^2 = m + n - 2\sqrt{mn}$, so the values of x are $\pm(\sqrt{m} \pm \sqrt{n})$.

   As μ is irreducible (given), it is the minimal polynomial over $\mathbb{Q}$ of each of these numbers.

8. Let μ be the minimal polynomial of α over K, so μ divides both f and g.

   μ is irreducible, hence separable, over K. Thus if μ had degree > 1 it would have a zero $\beta \neq \alpha$, which would also be a common zero of f and g. As this is not the case, $\partial\mu = 1$ so $\mu = t - \alpha$. As $\mu \in K[t]$ we must have $\alpha \in K$.

   Then $\mathrm{f} = (t - \alpha)\mathrm{h}$ for some h, which is in $K[t]$ by Exercises 1.3 Question 9, so f is reducible over K, as is g for the same reason.

9. The required polynomial has a factor $(t - 2^{1/3})^2$. Thus it is divisible by μ^2 where μ is the minimal polynomial of $2^{1/3}$, which is $t^3 - 2$.

Hence the required polynomial is $(t^3-2)^2$, i.e. t^6-4t^3+4. Its irreducible factors have no repeated zeros, so it is separable (but reducible) over $\mathbb{Q}$.

10. When $\mathrm{f} = t^6+2t^3+1 \in \mathbb{F}_3[t]$, $\mathrm{Df} = 6t^5+6t^2 = 0$ (the zero polynomial) since $6 = 0$ in $\mathbb{F}_3$.

    The proof of Proposition 1.17 uses the fact that if $\partial \mathrm{f} \geq 1$ then $\mathrm{Df} \neq 0$, but the above example shows that this is not so in general over a field of non-zero characteristic. Thus a different proof is need for finite fields; it uses properties that we have not covered in this module.