Q1 (i)(a) Bookwork

Suppose (∗) has a repeated root. Then the LHS factorizes as

$$t^3 + pt + q = (t-u)^2(t-v) \qquad \boxed{1}$$

where $u, v \in \mathbb{R}$ (possibly equal). Expanding out we have

$$2u + v = 0, \qquad 2uv + u^2 = p, \qquad -u^2v = q.$$

Eliminating v, this gives

$$p = -3u^2, \qquad q = 2u^3. \qquad \boxed{1}$$

To eliminate u, cube the first equation and square the second. We obtain

$$4p^3 + 27q^2 = 0. \qquad \boxed{1}$$

So if (∗) has repeated roots, the quantity $4p^3 + 27q^2$ is zero.

(b) Unseen Suppose (∗) has one real and two complex, non-real, roots. Then it factorizes as

$$t^3 + pt + q = (t-u)(t^2 + bt + c) \qquad \boxed{1}$$

where $b^2 - 4c < 0$. Expanding out we get

$$b - u = 0, \quad c - bu = p, \quad -cu = q, \qquad \boxed{1}$$

so

$$4p^3 + 27q^2 = 4(c - b^2) + 27b^2c^2 = 4c^3 + 15b^2c^2 + 12b^4c - 4b^6. \qquad \boxed{1}$$

This is the negative of

$$4b^6 - 12b^4c - 15b^2c^2 - 4c^3 = (b^2 - 4c)(4b^4 + 4b^2c + c^2). \qquad \boxed{2}$$

Now $4b^4 + 4b^2c + c^2 \geqslant 0$ and can only be zero if $b = c = 0$ and therefore $p = q = 0$, contradicting the assumption of non-real roots. $\boxed{1}$

Since $b^2 - 4c < 0$ we get $4p^3 + 27q^2 > 0$.

(ii) Bookwork

The characteristic of a field K is the least positive integer n such that $n1 = 0$. $\boxed{1}$ If no such n exists then K has characteristic zero. $\boxed{1}$

A homomorphism of fields is a map $\varphi\colon K \to L$ such that $\varphi(0_K) = 0_L$, $\varphi(1_K) = 1_L$, $\boxed{1}$ $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in K$. $\boxed{1}$

The degree of a homomorphism $\varphi\colon K \to L$ is the dimension of the vector space L over $\varphi(K)$. $\boxed{\text{1, any equivalent formulation acceptable}}$

An automorphism of fields is a homomorphism $\varphi\colon K \to L$ which is a bijection. $\boxed{1}$

An ideal in a ring R is a subset I which contains the zero element, is closed under addition, and is such that if $a \in R$ and $b \in I$ then $ab \in I$. $\boxed{3}$

(iii) Bookwork

(a) Take $a \in K$ with $a \neq 0$. Then a^{-1} exists and $aa^{-1} = 1_K$. So $\varphi(a)\varphi(a^{-1}) = \varphi(1_K) = 1_L$. In particular $\varphi(a) \neq 0_L$. $\boxed{2}$

(b) If $n \in \mathbb{N}$ and $n1_K \neq 0_K$ then $\varphi(n1_K) \neq 0_L$, by (a). $\boxed{1}$ And

$$\varphi(n1_K) = \varphi(1_K + \cdots + 1_K) \ (n \text{ times}) \ = 1_L + \cdots + 1_L = n1_L$$

so $n1_L \neq 0_L$. $\boxed{1}$ Likewise $n1_K = 0_K$ implies that $n1_L = 0_L$. So, for $n \in \mathbb{N}$,

$$n1_K \neq 0_K \text{ if and only if } n1_L \neq 0_L. \qquad \boxed{1}$$

It follows that K has characteristic 0 if and only if L has characteristic 0.

If K has characteristic p then $p1_K = 0_K$ but $n1_K \neq 0_K$ for $n = 1, \ldots, p-1$. So $p1_L = 0_L$ but $n1_L \neq 0_L$ for $n = 1, \ldots, p-1$. $\boxed{1}$ Therefore L has characteristic p. The converse is similar. $\boxed{1}$

2(a) Bookwork

A polynomial is primitive if there is no prime p which divides all its coefficients. Denote by π_p the canonical ring homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$. Then $q(x) \in \mathbb{Z}[x]$ is primitive if and only if $\pi_p(f(x)) \neq 0$ for all primes p. **2**

Consider a prime p. By the assumption we have $\pi_p(f(x)) \neq 0$ and $\pi_p(g(x)) \neq 0$. Since $\mathbb{F}_p$ is a field, we have $\pi_p(f(x))\pi_p(g(x)) \neq 0$. **1** Now $\pi_p(f(x)g(x)) = \pi_p(f(x))\pi_p(g(x))$, so $\pi_p(f(x)g(x)) \neq 0$. **1**

As this holds for all p it follows that $f(x)g(x)$ is primitive, as claimed. **1**

(b) Bookwork

Let u be the least common multiple of the denominators of the coefficients of f, or equivalently the smallest positive integer such that the polynomial $\overline{f}(x) = uf(x)$ lies in $\mathbb{Z}[x]$. **1** We claim that $\overline{f}(x)$ is primitive.

Indeed, if it were not primitive, there would be a prime p that divides all the coefficients of $\overline{f}(x)$, and then $\frac{1}{p}uf(x)$ would also be in $\mathbb{Z}[x]$, contradicting the definition of u. So $\overline{f}(x)$ must be primitive after all. **2**

Similarly, we can find an integer $v > 0$ such that the polynomial $\overline{g}(x) = vg(x)$ is integral and primitive.

Now put $\overline{q}(x) = \overline{f}(x)\overline{g}(x)$, and note from (a) that $\overline{q}(x)$ is primitive. **1**

On the other hand, we have $\overline{q}(x) = uvf(x)g(x) = uvq(x)$, with $uv \in \mathbb{N}$ and $q(x) \in \mathbb{Z}[x]$. It follows that any prime dividing uv divides all the coefficients of $\overline{q}(x)$, which is impossible because $\overline{q}(x)$ is primitive. **2**

It follows that there cannot be any primes dividing uv, so we must have $u = v = 1$. Thus $f(x) = \overline{f}(x) \in \mathbb{Z}[x]$ and $g(x) = \overline{g}(x) \in \mathbb{Z}[x]$ as claimed. **1**

(c) Standard type

The only quadratics over $\mathbb{F}_2$ are x^2, x^2+1, x^2+x and x^2+x+1. **2**

Of these we have that x^2, $x^2+1 = (x+1)^2$ and $x^2+x = x(x+1)$ are not irreducible. **1**

$p(x) := x^2+x+1$ has $p(0) = 1$ and $p(1) = 1$ so is irreducible over F_2. **1**

(d) Standard type

First, in $\mathbb{F}_2$ we have $f(0) = 1$ and $f(1) = 1$, so $f(x)$ has no roots, so it has no factors of degree one. **1** Thus, the only way it could factorise would be as an irreducible quadratic times an irreducible cubic. **1**

By long division over $\mathbb{F}_2$ we get

$$f(x) = (x^3+x^2)(x^2+x+1)+1, \qquad \boxed{2}$$

so $f(x)$ is not divisible by x^2+x+1. It is therefore irreducible as claimed. **1**

Now suppose there is a factorisation $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$, where $g(x)$ and $h(x)$ are monic. Then from (b) it follows that $g(x), h(x) \in \mathbb{Z}[x]$, so we can reduce everything modulo 2. **1**

We then have $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $\mathbb{F}_2[x]$, but $\overline{f}(x)$ is irreducible, so one of the factors must be equal to one, say $\overline{g}(x) = 1$. $\boxed{\mathbf{1}}$ As $g(x)$ is monic, the only way we can have $\overline{g}(x) = 1$ is if $g(x) = 1$. $\boxed{\mathbf{1}}$ We deduce that $f(x)$ is irreducible in $\mathbb{Q}[x]$, as claimed. $\boxed{\mathbf{1}}$

3 Bookwork

(a) We argue by induction on n.

If $n = 1$ then we have $b_1\theta_1(a) = 0$ for all $a \in L$, and we can take $a = 1$ to see that $b_1 = 0$; this starts the induction. $\boxed{1}$

Now suppose the result true for some specific $n > 1$. $\boxed{1}$ Fix some $t \in L$, and put $c_i = b_i(\theta_i(t) - \theta_n(t))$, $\boxed{1}$ so $c_n = 0$.

We claim that $\sum_{i=1}^{n-1} c_i\theta_i(a) = 0$ for all $a \in L$.

Indeed, the relation $\sum_{i=1}^{n} b_i\theta_i(a) = 0$ is valid for all $a \in L$, so it works for ta in place of a, which gives $\sum_{i=1}^{n} b_i\theta_i(t)\theta_i(a) = 0$. $\boxed{1}$

On the other hand, we can just multiply the relation $\sum_{i=1}^{n} b_i\theta_i(a) = 0$ by $\theta_n(t)$ to get $\sum_{i=1}^{n} b_i\theta_n(t)\theta_i(a) = 0$, $\boxed{1}$ and then subtract this from the previous relation to get $\sum_{i=1}^{n-1} c_i\theta_i(a) = 0$ as claimed. $\boxed{1}$

We deduce from the induction hypothesis that $c_1 = \cdots = c_{n-1} = 0$, so $b_i(\theta_i(t) - \theta_n(t)) = 0$ for all $i < n$ (and all $t \in L$, because t was arbitrary). $\boxed{1}$

By assumption the homomorphisms θ_i are all different, so for each $i < n$ we can choose $t_i \in L$ with $\theta_i(t_i) \neq \theta_n(t_i)$. We can then take $t = t_i$ in the relation $b_i(\theta_i(t) - \theta_n(t)) = 0$ to get $b_i = 0$. $\boxed{1}$

This shows that $b_1 = \cdots = b_{n-1} = 0$, so the relation $\sum_{i=1}^{n} b_i\theta_i(a)$ reduces to $b_n\theta_n(a) = 0$ for all a. $\boxed{1}$

Now take $a = 1$ to see that $b_n = 0$ as well. This completes the induction. $\boxed{1}$

(b)

Write $m = \deg(\varphi)$ and let $e_1, \cdots, e_m$ be a basis for L over $\varphi(K)$. $\boxed{1}$

Let $\theta_1, \ldots, \theta_n$ be the distinct elements of $E(\varphi, \psi)$.

Define $v_1, \ldots, v_n \in M^m$ by

$$v_i = (\theta_i(e_1), \ldots, \theta_i(e_m)). \qquad \boxed{1}$$

We claim that these n vectors are linearly independent over M.

To see this, consider a linear relation $b_1v_1 + \cdots + b_nv_n = 0$ with $b_1, \ldots, b_n \in M$. $\boxed{1}$ So $\sum_{i=1}^{n} b_i\theta_i(e_j) = 0$ for all j.

Now consider an arbitrary element $a \in L$. As the elements e_j give a basis for L over $\varphi(K)$, we can write $a = \sum_{j=1}^{m} \varphi(x_j)e_j$ for some $x_1, \ldots, x_m \in K$. $\boxed{1}$ We can then apply θ_i to this. Since $\theta_i\varphi = \psi$, we get

$$\theta_i(a) = \sum_{j=1}^{m} \psi(x_j)\theta_i(e_j). \qquad \boxed{2}$$

It follows that

$$\sum_{i=1}^{n} b_i\theta_i(a) = \sum_{i=1}^{n}\sum_{j=1}^{m} b_i\psi(x_j)\theta_i(e_j) = \sum_{j=1}^{m}\left(\psi(x_j)\sum_{i=1}^{n} b_i\theta_i(e_j)\right) = 0. \boxed{1}$$

By (a) we have $b_1 = \cdots = b_n = 0$. $\boxed{\mathbf{1}}$ We deduce that the vectors $v_1, \dots, v_n$ in M^m are linearly independent $\boxed{\mathbf{1}}$. The length of any linearly independent list is at most the dimension of the containing space, so we have $n \leqslant m$ $\boxed{\mathbf{1}}$; that is, $|E(\varphi, \psi)| \leqslant \deg(\varphi)$.

(c)

Let N/K be a field extension of finite degree. We say that N is *normal* over K if for every monic irreducible polynomial $f(x) \in K[x]$, either f has no roots in N or f splits properly over N $\boxed{\mathbf{3}}$.

Equivalently: for any other extension L/K, either $E_K(L, N) = \emptyset$ or $|E_K(L, N)| = [L : K]$ (where $E_K(L, N) = \{\varphi\colon L \to N \mid \varphi|_K = 1\}$). $\boxed{\mathbf{2}}$

Alternatively, it is equivalent to say that $|G(N/K)| = [N : K]$. $\boxed{\textbf{(2 also for this answer)}}$

4(a) Standard type.

The set

$$B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{7}, \sqrt{6}, \sqrt{14}, \sqrt{21}, \sqrt{42}\}$$

is a basis for L over $\mathbb{Q}$. $\boxed{\mathbf{3}}$

(b) Standard type.

We can define automorphisms $\varphi, \psi, \omega \in G(L/\mathbb{Q})$ by

$$\begin{array}{lll} \varphi(\sqrt{2}) = -\sqrt{2} & \varphi(\sqrt{3}) = \sqrt{3} & \varphi(\sqrt{7}) = \sqrt{7} \\ \psi(\sqrt{2}) = \sqrt{2} & \psi(\sqrt{3}) = -\sqrt{3} & \psi(\sqrt{7}) = \sqrt{7} \\ \omega(\sqrt{2}) = \sqrt{2} & \omega(\sqrt{3}) = \sqrt{3} & \omega(\sqrt{7}) = -\sqrt{7}. \qquad \boxed{\mathbf{3}} \end{array}$$

More explicitly, we have

$$\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{7} + e\sqrt{6} + f\sqrt{14} + g\sqrt{21} + h\sqrt{42}) = \\ a - b\sqrt{2} + c\sqrt{3} + d\sqrt{7} - e\sqrt{6} - f\sqrt{14} + g\sqrt{21} - h\sqrt{42}$$

and so on. These automorphisms commute with each other and satisfy $\varphi^2 = \psi^2 = \omega^2 = 1$. The full group is

$$G(L/\mathbb{Q}) = \{1,\ \varphi,\ \psi,\ \omega,\ \varphi\psi,\ \varphi\omega,\ \psi\omega,\ \varphi\psi\omega\} \cong C_2 \times C_2 \times C_2. \qquad \boxed{\mathbf{3}}$$

(c) Close to standard type.

H_i is the set of automorphisms $\theta \in G(L/\mathbb{Q})$ satisfying $\theta|_{K_i} = 1$. For example, this means that H_1 is the group of those $\theta \in G(L/K)$ for which $\theta(\sqrt{14}) = \sqrt{14}$, or equivalently $\theta(\sqrt{2})\theta(\sqrt{7}) = \sqrt{2}\sqrt{7}$. This gives the list

$$H_1 = \{1, \varphi\omega, \psi, \varphi\psi\omega\}. \qquad \boxed{\mathbf{2}}$$

Similarly, we have

$$\begin{aligned} H_2 &= \{1, \varphi\psi\omega\} \qquad \boxed{\mathbf{1}} \\ H_4 &= \{1, \varphi\psi, \varphi\omega, \psi\omega\}. \qquad \boxed{\mathbf{1}} \end{aligned}$$

For H_3, we note that any $\theta \in G(L/\mathbb{Q})$ has $\theta(\sqrt{2} + \sqrt{7}) = \pm\sqrt{2} \pm \sqrt{7}$. As $\sqrt{2}$ and $\sqrt{7}$ are linearly independent over $\mathbb{Q}$, we see that $\theta(\sqrt{2} + \sqrt{7})$ can only be equal to $\sqrt{2} + \sqrt{7}$ if $\theta(\sqrt{2}) = \sqrt{2}$ and $\theta(\sqrt{7}) = \sqrt{7}$ $\boxed{\mathbf{1}}$, which means that θ cannot involve φ or ω. $\boxed{\mathbf{1}}$ We conclude that

$$H_3 = \{1, \psi\}. \qquad \boxed{\mathbf{1}}$$

(d) Unseen

As the Galois correspondence is an order-reversing bijection, we have $K_1 \leqslant K_3$ iff $H_1 \geqslant H_3$, which is true by part (c) $\boxed{\mathbf{2}}$. More explicitly, we have

$$\sqrt{14} = \tfrac{1}{2}\,(\sqrt{2}+\sqrt{7})^2 - \tfrac{9}{2},$$

so $\sqrt{14} \in \mathbb{Q}(\sqrt{2}+\sqrt{7})$, so $K_1 = \mathbb{Q}(\sqrt{14}) \leqslant \mathbb{Q}(\sqrt{2}+\sqrt{7}) = K_3$. $\boxed{\mathbf{2}}$

(e) Unseen

If a field M (with $\mathbb{Q} < M < L$) corresponds to a subgroup $H \leqslant G(L/\mathbb{Q})$, we have

$$|H| = [L : M] = [L : \mathbb{Q}]/[M : \mathbb{Q}] = 8/[M : \mathbb{Q}]. \qquad \boxed{\mathbf{1}}$$

Thus, the intermediate fields with $[M : \mathbb{Q}] = 4$ are in bijective correspondence with subgroups of order 2 in $G(L/\mathbb{Q})$ $\boxed{\mathbf{2}}$.

There are 7 non-identity elements $\theta \in G(L/K)$ $\boxed{\mathbf{1}}$, and each of these satisfies $\theta^2 = 1$ so it gives a subgroup $\{1, \theta\}$ of order 2, and this gives all such subgroups. $\boxed{\mathbf{1}}$ Thus, there are 7 intermediate fields of degree 4 over $\mathbb{Q}$.

5 Standard type

(a) Use Eisenstein's criterion:

Let p be a prime number. Suppose that $q(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$ is such that

- All the coefficients $a_0, \ldots, a_{d-1}$ are integers, and are divisible by p. $\boxed{1}$
- a_0 is not divisible by p^2. $\boxed{1}$

Then $q(x)$ is irreducible over $\mathbb{Q}$. $\boxed{1}$

For the given polynomial, $f(x) = x^4 \pmod{2}$ and $f(0) \neq 0 \pmod{4}$ so Eisenstein's criterion applies and $f(x)$ is irreducible. $\boxed{2}$

(b) Note that $\alpha^2 + 4 = 3\sqrt{2} = \sqrt{18}$, and squaring again shows that $\alpha^4 + 8\alpha^2 + 16 = 18$, so $f(\alpha) = 0$. $\boxed{1}$

As $f(x)$ only involves even powers of x we have $f(-x) = f(x)$ and so $f(-\alpha) = 0$. $\boxed{1}$

Now put $\beta = \sqrt{-3\sqrt{2} - 4}$; the same argument shows that $f(\pm\beta) = 0$. We also have $(\alpha\beta)^2 = (3\sqrt{2} - 4)(-3\sqrt{2} - 4) = -2$, so $\beta = \pm\sqrt{-2}/\alpha$. $\boxed{3}$ It follows that the roots of $f(x)$ are as described, so the splitting field is $\mathbb{Q}(\alpha, \beta)$ $\boxed{1}$ $= \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}(\alpha, \sqrt{-2}) = M$ as claimed. $\boxed{1}$

Use of quadratic formula gets same marks

(c) We have $3\sqrt{2} - 4 \simeq 0.24 > 0$ so α is real, so $\mathbb{Q}(\alpha) \subseteq M \cap \mathbb{R}$. $\boxed{1}$ As $f(x)$ is irreducible, it must be the minimal polynomial for α, $\boxed{1}$ and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 4$. $\boxed{1}$ As $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ and $\sqrt{-2}$ is purely imaginary we see that $1, \sqrt{-2}$ is a basis for M over $\mathbb{Q}(\alpha)$, $\boxed{1}$ so $M \cap \mathbb{R} = \mathbb{Q}(\alpha)$ and $[M : \mathbb{Q}] = [M : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8$. $\boxed{1}$

(d) First let $\psi\colon M \to M$ be given by complex conjugation, so $\psi(\sqrt{-2}) = -\sqrt{-2}$ and $\psi(\alpha) = \alpha$. It is clear that $\psi^2 = 1$. $\boxed{1}$

Next, the Galois group of the splitting field of an irreducible polynomial always acts transitively on the roots, so we can find $\sigma \in G(M/\mathbb{Q})$ with $\sigma(\alpha) = \sqrt{-2}/\alpha$. $\boxed{1}$

Now σ must permute the roots of $x^2 + 2$, so $\sigma(\sqrt{-2}) = \pm\sqrt{-2}$. $\boxed{1}$ If the sign is positive we put $\varphi = \sigma\psi$, otherwise we put $\varphi = \sigma$. In either case we then have $\varphi(\alpha) = \sqrt{-2}/\alpha = \beta$ and $\varphi(\sqrt{-2}) = -\sqrt{-2}$. $\boxed{1}$ This means that

$$\varphi^2(\alpha) = \varphi(\sqrt{-2}/\alpha) = \varphi(\sqrt{-2})/\varphi(\alpha) = -\sqrt{-2}/(\sqrt{-2}/\alpha) = -\alpha$$

and $\varphi^2(\sqrt{-2}) = \sqrt{-2}$. It follows in turn that $\varphi^4 = 1$. $\boxed{1}$

We now have various different automorphisms, whose effect we can tabulate as follows:

	1	φ	φ^2	φ^3	ψ	$\varphi\psi$	$\varphi^2\psi$	$\varphi^3\psi$
α	α	β	$-\alpha$	$-\beta$	α	β	$-\alpha$	$-\beta$
β	β	$-\alpha$	$-\beta$	α	$-\beta$	α	β	$-\alpha$
$\sqrt{-2}$	$\sqrt{-2}$	$-\sqrt{-2}$	$\sqrt{-2}$	$-\sqrt{-2}$	$-\sqrt{-2}$	$\sqrt{-2}$	$-\sqrt{-2}$	$\sqrt{-2}$.

$\boxed{2}$

We see that the eight automorphisms listed are all different, but $|G(M/\mathbb{Q})| = [M : \mathbb{Q}] = 8$, so we have found all the automorphisms. $\boxed{\mathbf{1}}$