Q1 (i)(a) Bookwork Putting $u = \sqrt[3]{y} + \sqrt[3]{z}$ in $(*)$ we get

$$u^3 = y + 3\sqrt[3]{y^2 z} + 3\sqrt[3]{yz^2} + z = y + z + 3\sqrt[3]{yz}(\sqrt[3]{y} + \sqrt[3]{z}) = y + z + 3u\sqrt[3]{yz} \quad \boxed{2}$$

so $u^3 - 3u\sqrt[3]{yz} - (y+z) = 0$. Comparing this with $(*)$ we must have

$$p = -3\sqrt[3]{yz}, \qquad q = -(y+z). \quad \boxed{2}$$

(b) We now solve these for z. Put $y = -(q+z)$ into the first equation. We get

$$3\sqrt[3]{z}\sqrt[3]{(z+q)} = p. \quad \boxed{2}$$

Cubing gives $27z(z+q) = p^3$. This rearranges to $27z^2 + 27qz - p^3 = 0$. $\boxed{1}$

(c) We have converted the solution of the cubic into the solution of a quadratic. Solving in the usual way, we have

$$-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}. \quad \boxed{1}$$

Since $u = \sqrt[3]{y} + \sqrt[3]{z}$ and $y + z = -q$ we have

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}. \quad \boxed{2}$$

(ii) Bookwork

Suppose that x is a nonzero element of M; we need to show that x has an inverse in M. $\boxed{1}$

Write $d = \dim_K(M)$; this dimension is finite because M is a vector subspace of L. The elements $1, x, x^2, \dots, x^d$ are $d+1$ in number, so must be linearly dependent. That is, there are $a_0, a_1, \dots a_d \in K$, not all zero, such that

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d = 0. \quad \boxed{2}$$

So $I(x, K) \neq 0$, and there is therefore an irreducible monic polynomial $q(t) = \min(x, K)(t) = \sum_{i=0}^{D} b_i t^i$ say, with $q(x) = 0$. $\boxed{1}$

We claim that $q(0) \neq 0$. Indeed, if $q(0)$ were zero then t would be a nonconstant monic factor of the irreducible polynomial $q(t)$, and this would mean that t would have to equal $q(t)$, so the equation $q(x) = 0$ would give $x = 0$, contradicting our assumption that x is nonzero. $\boxed{2}$

Thus, the constant term $b_0 = q(0)$ is nonzero, and thus invertible in K. We now put $y = -\sum_{i=1}^{D} b_0^{-1} b_i x^{i-1} \in M$. $\boxed{1}$ The equation $\sum_{i=0}^{D} b_i x^i = 0$ can then be rearranged to give $xy = 1$, $\boxed{1}$ so y is the required inverse to x in M.

(iii) Unassigned exercise Suppose that $\sigma(i) = i$. Transitivity means that for any $j \in N$ we can choose $\tau \in A$ with $\tau(i) = j$. **1** As A is commutative we then have

$$\sigma(j) = \sigma(\tau(i)) = \tau(\sigma(i)) = \tau(i) = j. \qquad \boxed{1}$$

As j was arbitrary, this means that σ is the identity. **1**

Next, as A is transitive we can choose $\sigma_i \in A$ (for $i = 1, \ldots, N$) such that $\sigma_i(1) = i$. **1** Now let τ be any element of A. Put $i = \tau(1)$, and note that $\tau^{-1}\sigma_i$ sends 1 to 1. **1** By the first paragraph, this means that $\tau^{-1}\sigma_i = 1$, so $\tau = \sigma_i$. **1** This means that $A = \{\sigma_1, \ldots, \sigma_n\}$, and these elements are all different.

In particular $|A| = n$. **1**

Q2 (i) Bookwork The requirement that $\overline{\varphi} \circ \pi = \varphi$ forces us to define $\overline{\varphi}\colon R/I \to S$ by $\overline{\varphi}(a + I) = \varphi(a)$. [1] So if $\overline{\varphi}$ is a morphism, it is the unique such morphism. [1]

To show that this is well-defined, suppose that $a + I = b + I$. Then $a - b \in I$ and so $\varphi(a - b) = 0$. Therefore $\varphi(a) = \varphi(b)$. [2]

To show that $\overline{\varphi}$ is a morphism:

$$\begin{aligned}\overline{\varphi}((a + I) + (b + I)) &= \overline{\varphi}((a + b) + I) = \varphi(a + b) = \varphi(a) + \varphi(b) = \overline{\varphi}(a + I) + \overline{\varphi}(b + I),\\ \overline{\varphi}((a + I)(b + I)) &= \overline{\varphi}(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a + I)\overline{\varphi}(b + I),\\ \overline{\varphi}(1_R + I) &= \varphi(1_R) = 1_S. \qquad \boxed{3}\end{aligned}$$

Now assume that φ is surjective. Then $\overline{\varphi}$ is surjective because every $s \in S$ is $\varphi(a) = \overline{\varphi}(a + I)$ for some $a \in R$. [1]

Now assume that $\ker(\varphi) = I$. Suppose that $\overline{\varphi}(a + I) = 0$. Then $\varphi(a) = 0$ so $a \in I$ and therefore $a + I = 0 + I$. [2]

(ii)(a) Bookwork

$$E_K(L, M) = \{\theta\colon L \to M \mid \theta|_K = \mathrm{id}_K\}. \qquad \boxed{1}$$

(b) Bookwork Let d be the degree of q, or equivalently the degree of the homomorphism φ. [1] Let R be the set of roots of $(\widetilde{\psi}q)(t)$ in M.

We can write $q(t)$ in the form $q(t) = a_0 + a_1 t + \cdots + a_d t^d$, where $a_d = 1$ since $q(t)$ is monic. By definition we have $(\widetilde{\varphi}q)(\alpha) = 0$, or equivalently $\sum_i \varphi(a_i)\alpha^i = 0$. [1] Suppose that $\theta \in E(\varphi, \psi)$, so $\theta\varphi = \psi\colon K \to M$. We can then apply θ to the above equation to get

$$(\widetilde{\psi}q)(\theta(\alpha)) = \sum_i \psi(a_i)\theta(\alpha)^i = \theta(\sum_i a_i\alpha^i) = \theta(0) = 0,$$

so $\theta(\alpha) \in R$ [2]. This defines a map $P\, E(\varphi, \psi) \to R$ by $P(\theta) = \theta(\alpha)$. [1]

Now suppose we have two elements $\theta_0, \theta_1 \in E(\varphi, \psi)$ with $P(\theta_0) = P(\theta_1)$, so $\theta_0(\alpha) = \theta_1(\alpha) = \beta$ say. It follows from the result provided that every element $\sigma \in L$ can be written in the form $\sigma = \sum_{j=0}^{d-1} \varphi(b_j)\alpha^j$, for some elements $b_j \in K$. [1] Using $\theta_i(\varphi(b)) = \psi(b)$ and $\theta_i(\alpha) = \beta$ we deduce that $\theta_0(\sigma) = \sum_j \psi(b_j)\beta^j = \theta_1(\sigma)$. As σ was arbitrary this means that $\theta_0 = \theta_1$, so we see that P is injective. [2]

Finally, consider a general element $\beta \in R$, so β is a root of $(\widetilde{\psi}q)(t)$. We can then define a homomorphism $\lambda\, K[t] \to M$ by $\lambda(f(t)) = (\widetilde{\psi}f)(\beta)$, or more explicitly

$$\lambda(\sum_i b_i t^i) = \sum_i \psi(b_i)\beta^i. \qquad \boxed{1}$$

We then have $\lambda(q(t)) = 0$, so $\lambda(K[t].q(t)) = 0$. [1] There is therefore a homomorphism

$$\overline{\lambda}\colon K[t]/(K[t].q(t)) \to M, \qquad \boxed{1}$$

which we can compose with the inverse of the isomorphism $\overline{\chi}\colon K[t]/(K[t].q(t)) \to L$ to get a homomorphism $\theta = \overline{\lambda} \circ \overline{\chi}^{-1}\colon L \to M$ which clearly satisfies $P(\theta) = \beta$. [2] This means that P is also surjective, so it is a bijection. [1]

3(a) Bookwork Any one of:

- For every field L and homomorphism $\varphi\ K \to L$, we have either $|E(\varphi,\psi)| = 0$ or $|E(\varphi,\psi)| = \deg(\varphi)$.
- $|G(\psi)| = \deg(\psi)$.
- ψ is a proper splitting extension for some polynomial $f(t) \in K[t]$. **3**

(b) Bookwork

Theorem: Let M be a normal **1** extension of K, with Galois group $G = G(M/K)$.

(a) For any subgroup $H \leqslant G$, the set

$$L = M^H = \{a \in M \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$

is a subfield of M containing K, and M is normal over L with $G(M/L) = H$. **2**

(b) For any subfield $L \subseteq M$ containing K, the Galois group $H = G(M/L)$ is a subgroup of G and we have $M^H = L$. **2**

(c) If L and H are as above, then L is a normal extension of K if and only if H is a normal subgroup of G, and if so, then $G(L/K) = G/H$. **2**

(c) Unseen, standard type

Since $G(L/\mathbb{Q})$ is isomorphic to $C_2 \times C_2$, there are elements ρ and σ such that $\rho^2 = \sigma^2 = 1$ and $\rho\sigma = \sigma\rho$ and then

$$G := G(L/K) = \{1, \rho, \sigma, \rho\sigma\}. \qquad \mathbf{1}$$

Each element of order 2 in G defines a subgroup of G; write

$$A = \{1, \rho\}, \qquad B = \{1, \sigma\}, \qquad C = \{1, \rho\sigma\}. \qquad \mathbf{1}$$

Define subfields of L by

$$M = L^A, \qquad N = L^B, \qquad P = L^C. \qquad \mathbf{1}$$

Then A, B and C are the only proper nontrivial subgroups of G, so by (b) M, N and P are the only fields strictly between $\mathbb{Q}$ and L. **1** As G is abelian, all subgroups are normal, so M, N and P are normal over $\mathbb{Q}$, **1** with Galois groups G/A, G/B and G/C respectively. Each of these has order 2.

As $\sigma \notin A$, we see that σ acts nontrivially on M, so we can choose $\mu \in M$ with $\sigma(\mu) \neq \mu$ **1**. It follows that the element $\alpha = \mu - \sigma(\mu)$ is nonzero, and it satisfies $\sigma(\alpha) = -\alpha$ **1**. It follows that $\alpha \notin \mathbb{Q}$, and $[M : \mathbb{Q}] = |G/A| = 2$, so 1 and α must give a basis for M over $\mathbb{Q}$, so $M = \mathbb{Q}(\alpha)$. **1**

We also have $\sigma(\alpha^2) = \alpha^2$, and so $\alpha^2 \in M^{G/A} = \mathbb{Q}$. Similarly, there is an element $\beta \in N$ such that $\{1, \beta\}$ is a basis for N over $\mathbb{Q}$, and $\rho(\beta) = -\beta$, and $\beta^2 \in \mathbb{Q}$. Note that $\rho(\alpha) = \alpha$

(as $\alpha \in M$) and $\sigma(\beta) = \beta$ (as $\beta \in N$). It follows that $\rho(\sigma(\alpha\beta)) = (-\alpha)(-\beta) = \alpha\beta$, so $\alpha\beta \in P$. **[1]**

We next claim that $\{1, \alpha, \beta, \alpha\beta\}$ is linearly independent over $\mathbb{Q}$. Suppose that

$$w + x\alpha + y\beta + z\alpha\beta = 0$$

for some $w, x, y, z \in \mathbb{Q}$. Applying σ we get

$$w - x\alpha + y\beta - z\alpha\beta = 0.$$

Applying ρ we get

$$w + x\alpha - y\beta - z\alpha\beta = 0.$$

Applying $\sigma\rho$ we get

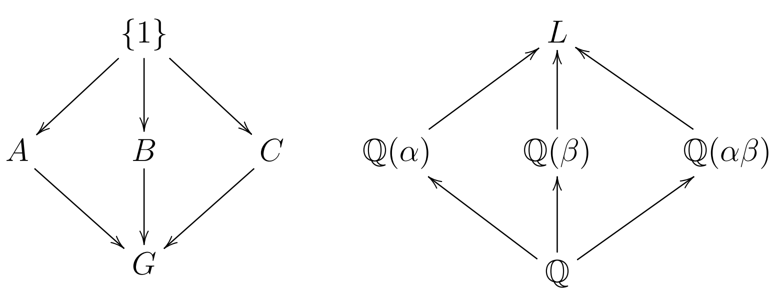
$$w - x\alpha - y\beta + z\alpha\beta = 0.$$ **[2]**

Adding the first equation to each of the others in turn we get

$$2w + 2y\beta = 0, \qquad 2w + 2x\alpha = 0, \qquad 2w + 2z\alpha\beta = 0.$$

Can cancel 2s since we are over $\mathbb{Q}$. So $y\beta = -w \in \mathbb{Q}$ and therefore $y = 0$. Similarly $x = 0$ and $z = 0$. Finally $w = 0$. **[1]**

Now since L is normal **[1]**, $\dim_{\mathbb{Q}}(L) = |G| = 4$, so $\{1, \alpha, \beta, \alpha\beta\}$ is a basis.



[2]

4 Unseen, standard type

(a) The roots of $f(t)$ are $\pm\alpha$ and $\pm i\alpha$ **2**. Thus $\mathbb{Q}(\alpha, i) \subseteq L$. Also $f(t)$ splits in L and the splitting is proper. **2** Since L is a proper splitting field for a polynomial, it is normal. **1**

(b) In general for field extensions $K \subseteq M \subseteq L$ of finite degree, **1**

$$[L : M][M : K] = [L : K]. \qquad (*)$$ **1**

Write $M = \mathbb{Q}(\alpha)$. To find $[M : \mathbb{Q}]$ note first that $f(t)$ is irreducible by Eisenstein's Criterion **1 (statement not required)**. Hence it is the minimal polynomial of α over $\mathbb{Q}$ **1** and so $[M : \mathbb{Q}] = 4$. **1**

Now consider $[\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)]$. The minimal polynomial of i over $\mathbb{Q}(\alpha)$ is $g(t) = t^2 + 1$ since $g(i) = 0$ but $i \notin \mathbb{Q}(\alpha)$. **1** So $[\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)] = 2$.

By $(*)$ we have $[L : \mathbb{Q}] = 8$. **1**

(c) A basis for L over $\mathbb{Q}$ is $1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3$. **1** From the given values and the fact that $\sigma \in G(L/\mathbb{Q})$ we have that σ acts on the basis elements by

1	α	α^2	α^3	i	$i\alpha$	$i\alpha^2$	$i\alpha^3$
1	$i\alpha$	$-\alpha^2$	$-i\alpha^3$	i	$-\alpha$	$-i\alpha^2$	α^3

1

There is a unique such linear map with these values. It remains to check that it is a homomorphism of fields. We check a nontrivial case. For example:

$$\sigma(\alpha)\sigma(\alpha^3) = (i\alpha)(-i\alpha^3) = \alpha^4 = 2 = \sigma(2) = \sigma(\alpha\alpha^3).$$ **1**

An element of $G(L/\mathbb{Q})$ is determined by its values on α and i. **1** For powers of σ we have

	α	i
σ	$i\alpha$	i
σ^2	$-\alpha$	i
σ^3	$-i\alpha$	i
σ^4	α	i

2

For powers of τ we have

	α	i
τ	α	$-i$
τ^2	α	i

1

Next,

	id	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
α	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

2

These are all distinct, so are the eight elements of $G(L/\mathbb{Q})$. **1**

(d) Calculate $\tau\sigma$. We find that

$$\tau\sigma(\alpha) = \tau(i\alpha) = \tau(i)\tau(\alpha) = -i\alpha, \qquad \tau\sigma(i) = \tau(i) = -i,$$

so $\tau\sigma = \sigma^3\tau$. **2** Together with the facts that σ has order 4 and τ has order 2, this shows that $G(L/\mathbb{Q})$ is the dihedral group D_8. **1**

5 Unseen, standard type

(a) Suppose $f(t)$ is reducible over $\mathbb{Q}$. Then it has a linear factor $t-a$ and by Gauss' Lemma **1**, $a \in \mathbb{Z}$. However, $f(t) \neq 0$ for $t = 0, \pm 1, \pm 2$ by calculation. **1** For $t > 2$ we have $f(t) > 0$ and for $t < -2$ we have $f(t) < 0$. (Put $t = 2 + u$, etc.) **1** Therefore $f(t)$ does not have a linear factor, and therefore is irreducible.

(b) $\alpha^3 = \xi^3 + 3\xi + 3\xi^{-1} + \xi^{-3}$ so

$$\alpha^3 - 3\alpha = \xi^3 + \xi^{-3} = e^{\pi i/3} + e^{-\pi i/3} = 2\cos\tfrac{\pi}{3} = 1.$$

Likewise $\beta^3 = -\xi^6 - 3\xi^2 - 3\xi^{-2} - \xi^{-6}$ so

$$\beta^3 - 3\beta = -\xi^6 - \xi^{-6} = -e^{2\pi i/3} - e^{-2\pi i/3} = -2\cos\tfrac{2\pi}{3} = 1,$$

and $\gamma^3 = -\xi^{12} - 3\xi^4 - 3\xi^{-4} - \xi^{-12}$ so

$$\gamma^3 - 3\gamma = -\xi^{12} - \xi^{-12} = -e^{4\pi i/3} - e^{-4\pi i/3} = -2\cos\tfrac{4\pi}{3} = 1,$$

3 for method, 3 for accuracy

(c)

$$\beta^2 = \xi^4 + 2 + \xi^{-4} = -\gamma + 2. \qquad \boxed{1}$$

Next, $\gamma^2 = \xi^8 + 2 + \xi^{-8}$ and $\xi^9 = e^{\pi i} = -1$ so $\xi^8 = -\xi^{-1}$ and $\xi^{-8} = -\xi$. **1** So

$$\gamma^2 = -\xi - \xi^{-1} + 2 = 2 - \alpha. \qquad \boxed{1}$$

Likewise

$$\alpha^2 = \xi^2 + 2 + \xi^{-2} = -\beta + 2. \qquad \boxed{1}$$

Since $f(t)$ is irreducible, the splitting field is $\mathbb{Q}(\alpha, \beta, \gamma)$. **1**

From $\beta^2 = 2 - \gamma$ it follows that $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta)$

And from $\gamma^2 = 2 - \alpha$ it follows that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma)$.

Lastly, from $\alpha^2 = 2 - \beta$ it follows that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$.

So we have $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ and therefore $\mathbb{Q}(\alpha) = \mathbb{Q}(\gamma) = \mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha)$. **3**

(d) Since $\mathbb{Q}(\alpha)$ is the proper splitting field for a polynomial it is a normal extension of $\mathbb{Q}$. **1** Hence there is $\sigma \in G := G(\mathbb{Q}(\alpha)/\mathbb{Q})$ such that $\sigma(\alpha) = \beta$. **2**

It follows that $\sigma(\beta) = \sigma(2 - \alpha^2) = 2 - \beta^2 = \gamma$. **1** Therefore σ cycles the roots $\alpha \mapsto \beta \mapsto \gamma$ **1** and the subgroup $\{\mathrm{id}, \sigma, \sigma^2\}$ has order 3.

Since $\mathbb{Q}(\alpha)$ is normal, $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. **1** Now $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ **1**. Hence $G = \{\mathrm{id}, \sigma, \sigma^2\}$ and is the cyclic group of order 3. **1**