1 Easy

(a) $\varphi\colon\ L \to L$ is a homomorphism of fields, a bijection, and $\varphi(a) = a$ for all $a \in K$. **3**

(b)(i) The *Galois group* $\mathrm{Gal}(L/K)$ is the set of K-automorphisms of L with composition as the group operation. **2**

(ii) A field extension L/K is *Galois* if $[L : K] = |\,\mathrm{Gal}(L/K)|$. **2**

(c)(i) There is only one element, the identity.

For φ any automorphism, $\varphi(\sqrt[3]{2})$ must again be a cube root of unity. But $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of $\mathbb{R}$ and so $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. **3**

(c)(ii) There are two elements, the identity and the map

$$\varphi(a + b\omega) = a + b\omega^2.$$

This is (a restriction of) complex conjugation so is a field automorphism.

These are the only possibilities because any φ must leave each rational fixed and the only possibilities for $\varphi(\omega)$ are ω and the other nonrational cube root, ω^2. **3**

(d) $\mathbb{Q}(\sqrt[3]{2}, \omega)$. **3**

(e)(i) Try $\gamma = \sqrt{3} + \sqrt{7}$. Clearly $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Now

$$\gamma^3 = 3\sqrt{3} + 3 \times 3\sqrt{7} + 3 \times 7\sqrt{3} + 7\sqrt{7} = 24\sqrt{3} + 16\sqrt{7} = 16\gamma + 8\sqrt{3}$$

so

$$\sqrt{3} = \tfrac{1}{8}(\gamma^3 - 16\gamma) \in \mathbb{Q}(\gamma).$$

Similarly $24\sqrt{3} + 16\sqrt{7} = 24\gamma - 8\sqrt{7}$ so

$$\sqrt{7} = -\tfrac{1}{8}(\gamma^3 - 24\gamma) \in \mathbb{Q}(\gamma).$$

So $\mathbb{Q}(\sqrt{3}, \sqrt{7}) \subseteq \mathbb{Q}(\gamma)$. **4**

(e)(ii) $x^4 - 20x^2 + 16$. **3**

(f) G is *soluble* if there is a finite chain

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = \{1\}$$

such that each G_{i+1} is normal in G_i **1** and each quotient is abelian. **1**

2(a) Bookwork. Easy

$$\lambda_n(x) = \prod_{\text{primitive } n\text{th roots of unity}} (x - \zeta). \qquad \boxed{\mathbf{3}}$$

(b) Unseen. Let ζ be any primitive 15th root of unity. Then ζ^5 will be a cube root of unity. But it will not be 1 since, if it were, ζ would not be primitive as a 15th root.

So ζ^5 must be a primitive cube root of unity and therefore satisfies $x^2 + x + 1 = 0$. That is, $\zeta^{10} + \zeta^5 + 1 = 0$. $\boxed{\mathbf{3}}$

(c) Unseen. Easy. $\boxed{\mathbf{3}}$

(d) Unseen. The integers $1 \leqslant k \leqslant 15$ which are coprime to 15 are $1, 2, 4, 7, 8, 11, 13, 14$. There are eight such integers, so $\lambda_{15}(x)$ has degree eight. By (a), $\lambda_{15}(x)$ divides $x^{10}+x^5+1$. The factor $x^2 + x + 1$ in (b) is $\lambda_3(x)$. So the remaining factor must be the product of $(x - \zeta)$ for all primitive 15th roots of unity ζ. $\boxed{\mathbf{3}}$

3. Bookwork.

(a) TPE: Let $K \subseteq L$ be a field extension. Then $L = K(\gamma)$ for some element $\gamma \in L$. **2**

(b) APR: Let $K \subseteq L$ be a field extension, and let $\alpha \in L$ be algebraic over K **1** with minimal polynomial $f(x) \in K[x]$ over K **1**. If $\theta \in \mathrm{Gal}(L/K)$, then $\theta(\alpha)$ is also a root of $f(x)$. **2**

(c) By the TPE, there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K. Then

- $[L : K]$ is equal to the degree of f, **1** and
- $|\mathrm{Gal}(L/K)|$ is equal to the number of distinct roots of f in L. **1**

So $[L : K] = |\mathrm{Gal}(L/K)|$ implies that the number of roots of f in L is equal to the degree of f; that is, f factorises over L into distinct linear factors. Thus L is the splitting field of $f(x)$ over K. **2**

(d) L is the splitting field of some polynomial $f(x) \in K[x]$ by (c). Since $K \subseteq M$ we have $f(x) \in M[x]$. Now L splits $f(x)$ and is generated over K by the roots, so it is also generated over M by the roots. Thus L is the splitting field for $f(x)$ over M, and is therefore Galois. **4**

(e) By the TPE there is $\alpha \in M$ such that $M = K(\alpha)$ and M is the splitting field for the irreducible polynomial $m_\alpha(x)$. **2** Now φ must map α to another root of $m_\alpha(x)$ by the APR but this root, β say, is also in M, because M splits $m_\alpha(x)$. It then follows that $\varphi(M) \subseteq M$. **2** Similarly $\varphi^{-1}(M) \subseteq M$, so $\varphi(M) = M$. **1**

(f) Bookwork, Hard Take $\varphi \in \mathrm{Gal}(L/K)$ and $\theta \in \mathrm{Gal}(L/M)$. Since M/K is Galois, $\varphi(M) = M$ by (e). Thus $\varphi(\theta(\varphi^{-1}(m))) = \varphi(\theta(m'))$ where $m' = \varphi^{-1}(m) \in M$ and so

$$\varphi(\theta(\varphi^{-1}(m))) = \varphi(\theta(m')) = \varphi(m') = m.$$

That is, $\varphi \circ \theta \circ \varphi^{-1}$ fixes every element of M. So $\varphi \circ \theta \circ \varphi^{-1} \in \mathrm{Gal}(L/M)$, and therefore $\mathrm{Gal}(L/M)$ is normal in $\mathrm{Gal}(L/K)$. **4**

Now define a map

$$\Phi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K) \qquad \theta \mapsto \theta|_M. \qquad \boxed{2}$$

Since $\theta(M) = M$, we have $\theta|_M \in \mathrm{Gal}(M/K)$, as required. The map Φ is easily seen to be a group homomorphism, and its kernel consists of all θ such that $\theta|_M(m) = m$ for all $m \in M$, so is $\mathrm{Gal}(L/M)$. **3** Then the first isomorphism theorem for groups gives:

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Im}\,\Phi \subseteq \mathrm{Gal}(M/K). \qquad \boxed{1}$$

Now the order of the quotient group is

$$\frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L : K]}{[L : M]} \qquad \boxed{1}$$

since L/K and L/M are Galois, **2** and

$$\frac{[L:K]}{[L:M]} = [M:K] = |\mathrm{Gal}(M/K)|. \qquad \mathbf{2}$$

Therefore $\mathrm{Im}\,\Phi = \mathrm{Gal}(M/K)$. **1**

FIT: If $\varphi\colon G \to H$ is a group homomorphism then there is a unique group isomorphism $\overline{\varphi}\colon G/\ker(\varphi) \to \mathrm{Im}\,(\varphi)$ such that $\varphi(g) = \overline{\varphi}(g\ker(\varphi))$ for all $g \in G$. **2**

Degree Theorem: If $K \subseteq M \subseteq L$ are field extensions, then $[L:K] = [L:M]\,[M:K]$. **1**

4. Standard type.

(a) ξ is a primitive 7th root of unity and 7 is prime, so

$$1+\xi+\xi^2+\xi^3+\xi^4+\xi^5+\xi^6=0. \qquad \boxed{2}$$

Next, we have

$$\begin{aligned}\beta &= \xi+\xi^6\\ \beta^2 &= \xi^2+2\xi^7+\xi^{12}\\ &= 2+\xi^2+\xi^5\\ \beta^3 &= \xi^3+3\xi^8+3\xi^{13}+\xi^{18}\\ &= 3\xi+\xi^3+\xi^4+3\xi^6,\end{aligned}$$

so

$$\beta^3+\beta^2-2\beta-1=1+\xi+\xi^2+\xi^3+\xi^4+\xi^5+\xi^6=0,$$

so x^3+x^2-2x-1 is the required cubic polynomial for β. $\boxed{3}$

(b) Similarly, we have

$$\begin{aligned}\gamma^2 &= (\xi+\xi^2+\xi^4)^2\\ &= \xi^2+\xi^4+\xi^8+2(\xi^3+\xi^5+\xi^6)\\ &= \xi+\xi^2+2\xi^3+\xi^4+2\xi^5+2\xi^6\\ \gamma^2+\gamma+2 &= 2+2\xi+2\xi^2+2\xi^3+2\xi^4+2\xi^5+2\xi^6=0,\end{aligned}$$

so x^2+x+2 is the required quadratic polynomial for γ. $\boxed{3}$

(c) Using the quadratic formula we deduce that

$$\gamma=(-1\pm\sqrt{-7})/2 \quad \text{so} \quad \sqrt{-7}=\pm(1+2\gamma)\in\mathbb{Q}(\gamma). \qquad \boxed{2}$$

(d) The elements of $G(\mathbb{Q}(\xi)/\mathbb{Q})$ are the automorphisms φ_k given by $\xi\mapsto\xi^k$, where $0<k<7$. $\boxed{1}$ Since 7 is prime, k and 7 are coprime for all such k. Thus, we have

$$G(\mathbb{Q}(\xi)/\mathbb{Q})=\{\varphi_1=\mathrm{id},\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6\}. \qquad \boxed{2}$$

(e) The powers of 3 mod 7 are $1,3,2,6,4$ and 5, so the powers of φ_3 are $\varphi_1,\varphi_3,\varphi_2,\varphi_6,\varphi_4$ and φ_5. Thus, the group $G(\mathbb{Q}(\xi)/\mathbb{Q})$ is cyclic of order 6, $\boxed{1}$ generated by $\theta=\varphi_3$. $\boxed{2}$

Any finite cyclic group has precisely one subgroup of each order dividing the group order. Thus, the subgroups are

$$\begin{aligned}C_1 &= \{1\}\\ C_2 &= \{1,\theta^3\}\\ C_3 &= \{1,\theta^2,\theta^4\}\\ C_6 &= \{1,\theta,\theta^2,\theta^3,\theta^4,\theta^5\}=G(\mathbb{Q}(\xi)/\mathbb{Q}). \qquad \boxed{2}\end{aligned}$$

The lattices of subgroups and subfields are as follows:

4 for subgroups, 3 for subfields