[B]=bookwork, [S]=seen, [P]=partially seen, [U]=unseen

1. Suppose that $L : K$ is a field extension with $K \subseteq L$.

(2+1+2+3+3+2+4=17 marks)

(a) (i) State what it means for $\alpha \in L$ to be algebraic over K.
Solution: [B] α is algebraic over K when α is a root of a (nonzero) polynomial over K.

(ii) State what it means for L to be algebraic over K.
Solution: [B] L is algebraic over K if every element of L is algebraic over K.

(iii) For $\alpha \in L$, give the definitions of $K[\alpha]$ and $K(\alpha)$.
Solution: [B] $K[\alpha]$ is the smallest subring of L containing K and α. $K(\alpha)$ is the smallest subfield of L containing K and α.

(iv) For $\alpha \in L$, state when $K[\alpha] = K(\alpha)$.
Solution: [B] $K[\alpha] = K(\alpha)$ exactly when α is algebraic over K.

(v) Suppose that $\alpha \in L$ is algebraic over K. Define $m_\alpha(K)$, the minimal polynomial of α over K.
Solution: [B] $m_\alpha(K)$ is the [unique] monic irreducible polynomial over K for which α is a root.
[Equivalently, $m_\alpha(K)$ is the monic generator of the ideal $\{f \in K[t] : \ f(\alpha) = 0 \}$.]

(vi) Suppose that $0 \neq \alpha \in L$ is algebraic over K, and let a_0 denote the constant term of $m_\alpha(K)$. Briefly explain why $a_0 \neq 0$.
Solution: [P] Say $m_\alpha(K) \in K[t]$. [Since $0 \neq \alpha$, $m_\alpha(K) \neq t$.] If $a_0 = 0$ then $m_\alpha(K)/t$ is a nonzero polynomial over K for which α is a root, contradicting that $m_\alpha(K)$ is irreducible over K.

(vii) Suppose that $0 \neq \alpha \in L$ is algebraic over K. Show that $\alpha^{-1} \in K[\alpha]$.
Solution: [S] Write $m_\alpha(K) = a_0 + a_1X + \cdots + a_nX^n$ (so $a_0, \ldots, a_n \in K$ and $a_n = 1$). Since α is a root of $m_\alpha(K)$, we have

$$a_0 = -(a_1 + a_2\alpha + \cdots + a_n\alpha^{n-1})\alpha$$

and since $a_0 \neq 0$ we have

$$1 = -a_0^{-1}(a_1 + a_2\alpha + \cdots + a_n\alpha^{n-1})\alpha.$$

Thus $-a_0^{-1}(a_1 + a_2\alpha + \cdots + a_n\alpha^{n-1}) = \alpha^{-1}$, and as $a_0, \ldots, a_n \in K$, we have that α^{-1} is a K-linear combination of non-negative powers of α, i.e. $\alpha^{-1} \in K[\alpha]$.

(b) **(3+5=8 marks)**

(i) State the Tower Law.
Solution: [B] For $M : L$ and $L : K$ field extensions, we have $[M : L][L : K] = [M : K]$.

(ii) Suppose that $\alpha, \beta \in L$ are algebraic over K. Show that $\alpha + \beta$ is algebraic over K.
Solution: [S] Since α, β are algebraic over K, we know that $[K(\alpha) : K] < \infty$ and $[K(\beta) : K] < \infty$. Also, $m_\beta(K) \in K(\alpha)[X]$ [since $K \subseteq K(\alpha)$]. So β is algebraic over $K(\alpha)$ and hence $[K(\alpha, \beta) : K(\alpha)] < \infty$. Therefore $[K(\alpha, \beta) : K] < \infty$ by the Tower Law. We have $\alpha + \beta \in K(\alpha, \beta)$, so $K(\alpha, \beta) \supseteq K(\alpha + \beta) \supseteq K$. Hence, again by the Tower Law, we have

$$[K(\alpha, \beta) : K(\alpha + \beta)][K(\alpha + \beta) : K] = [K(\alpha, \beta) : K] < \infty$$

and so we must have $[K(\alpha + \beta) : K] < \infty$. This means that $\alpha + \beta$ is algebraic over K.

2. Suppose that K is a field.

(a) **(2+5=7 marks)**

(i) Define what it means for a field to be an algebraic closure of K.
Solution: [B] $\overline{K}$ is an algebraic closure of K if it is a maximal algebraic extension of K.

(ii) Suppose that L is a field so that $K \subseteq L \subseteq \overline{K}$ where $\overline{K}$ denotes an algebraic closure of K. Further, suppose that $\alpha, \beta \in L$ so that there is a K-homomorphism $\tau : K(\alpha) \to K(\beta)$ with $\tau(\alpha) = \beta$. Show that $m_\alpha(K) = m_\beta(K)$.
Solution: [S] Write $m_\alpha(K) = a_0 + a_1 t + \cdots + a_d t^d$ where $a_0, \ldots, a_d \in K$ with $a_d = 1$. Then $a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0$, so

$$0 = \tau(0) = \tau(a_0 + a_1\alpha + \cdots + a_d\alpha^d) = a_0 + a_1\beta + \cdots + a_d\beta^d$$

(since τ is a homomorphism leaving K pointwise fixed, and $\tau(\alpha) = \beta$). Therefore β is a root of $m_\alpha(K)$, which is monic [recall that $\tau(1) = 1$] and irreducible over K. Hence $m_\alpha(K)$ must be the minimal polynomial of β.

(b) **(2+2+4+5=13 marks)**
Suppose that $K \subseteq \overline{K}$ and $\alpha \in \overline{K}$ where $\overline{K}$ denotes an algebraic closure of K.

(i) Define what it means for α to be separable over K.
Solution: [B] α is separable over K if $m_\alpha(K)$ has d distinct roots in $\overline{K}$ where $d = \deg m_\alpha(K)$.

(ii) Present a basis for $K(\alpha)$ as a vector space over K.
Solution: [B] With $d = \deg m_\alpha(K)$, $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis for $K(\alpha)$ as a vector space over K.

(iii) Let $\sigma : K \to \overline{K}$ denote the inclusion map (so for every $\gamma \in K$, we have $\sigma(\gamma) = \gamma$). Precisely describe how to extend σ to a homomorphism $\tau : K(\alpha) \to \overline{K}$ and briefly explain why τ is well-defined. (You do not need to verify that τ is indeed a homomorphism.)
Solution: [S] Let $\beta \in \overline{K}$ be a root of $m_\alpha(K)$. With $d = \deg m_\alpha(K)$, by (ii) we know that for any $\gamma \in K(\alpha)$, there are (unique) $c_0, c_1, \ldots, c_{d-1} \in K$ so that

$$\gamma = c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}.$$

Define $\tau : K(\alpha) \to \overline{K}$ by

$$\tau(\gamma) = c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}.$$

τ is well-defined because the choice of γ uniquely determines $c_0, \ldots, c_{d-1} \in K$.

(iv) Show that the number of ways one can construct such τ (as in (iii)) is $[K(\alpha) : K]$ if α is separable over K, and less than $[K(\alpha) : K]$ if α is not separable over K.
Solution: [S] By (a)(ii), such τ needs to satisfy $\tau(\alpha) = \beta$ where $\beta \in \overline{K}$ is a root of $m_\alpha(K)$. So in (b)(iii), the number of choices we have for β is the number of (distinct) roots of $m_\alpha(K)$ in $\overline{K}$. We know that $[K(\alpha) : K] = d = \deg m_\alpha(K)$, and $m_\alpha(K)$ has at most d distinct roots since $K[t]$ is a UFD. When α is separable over K, $m_\alpha(K)$ has d distinct roots, and when α is not separable over K, $m_\alpha(K)$ has fewer than d distinct roots. [Hence the number of τ is $[K(\alpha) : K]$ when α is separable over K, and the number of τ is less than $[K(\alpha) : K]$ when α is not separable over K.]

(c) **(5 marks)** Suppose that p is prime, and $g \in \mathbb{F}_p[t]$ is irreducible of degree $d > 1$. Suppose that $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ and $\alpha \in \overline{\mathbb{F}}_p$ so that α is a root of g. Show that α^p is a root of g and that $\alpha^p \neq \alpha$.

Solution: [P] Write $g = c_0 + c_1 t + \cdots + c_d t^d$ [where $c_0, \ldots, c_d \in \mathbb{F}_p$]. So we have

$$g(\alpha^p) = c_0 + c_1\alpha^p + \cdots + c_d(\alpha^p)^d$$

and

$$(g(\alpha))^p = (c_0 + c_1 t + \cdots + c_d t^d)^p = c_0^p + c_1^p\alpha^p + \cdots + c_d^p(\alpha^d)^p$$

since $\mathbb{F}_p$ has characteristic p and so for $0 < k < p$, the binomial coefficient $\binom{p}{k} = 0$ in $\mathbb{F}_p$.

To see that $\alpha^p \neq \alpha$, we note that every element of $\mathbb{F}_p$ is a root of $t^p - t$ [by Fermat's Little Theorem, or by the theorem describing the fixed field of the Frobenious map]. Since $\deg g > 1$, we know that $\alpha \notin \mathbb{F}_p$, and as $t^p - t$ can have at most p roots in $\overline{\mathbb{F}}_p$, α cannot be a root of $t^p - t$ (and hence $\alpha^p \neq \alpha$).

3. Suppose that K, L are fields with $K \subseteq L$.

(a) **(2+1+2=5 marks)** Suppose that K, L are fields with $K \subseteq L$.

(i) Define what it means for $f \in K[t]$ to split over L.
Solution: [B] f splits over L if f factors as a product of linear factors in $L[t]$.

(ii) Define what it means for $L : K$ to be a splitting field extension for $f \in K[t]$.
Solution: [B] $L : K$ is a minimal field extension over which f splits.

(iii) Define what it means for $L : K$ to be a simple extension.
Solution: [B] $L : K$ is a simple extension if there is some $\gamma \in L$ so that $L = K(\gamma)$.

(b) **(15+5=20 marks)**

Indicate whether each of the following statements is always true or can be false (1 mark for each correct answer). For **5** of the statements you identify as false, provide a short justification (1 mark for each correct justification).

(i) Suppose that $\gamma \in \mathbb{C}$ is transcendental over $\mathbb{Q}$. Then there exist infinitely many fields M with $\mathbb{Q} \subseteq M \subseteq \mathbb{Q}(\gamma)$.
Solution: [B] True

(ii) There is a normal extension $L : K$ with some $\alpha \in L$ so that $m_\alpha(K)$ does not split over L.
Solution: [B] False. By the definition of a normal extension $L : K$, when $\alpha \in L$, $m_\alpha(K)$ must split over L.

(iii) Suppose that $L : K$ is a field extension with $K \subseteq L$, $\alpha \in L$, and $E_\alpha : K[t] \to L$ the evaluation map. Then α is transcendental over K if and only if E_α is injective.
Solution: [P] True.

(iv) Suppose that K, M, L are fields with $K \subseteq M \subseteq L$ and $L : K$ a Galois extension. Then $M : K$ is a Galois extension.
Solution: [P] False. Take $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt[4]{2})$, $L = M(i)$ (where $i = \sqrt{-1}$). Then the roots in $\mathbb{C}$ of $m_\alpha(\mathbb{Q})$ are $\pm\alpha, \pm i\alpha$. However, $\pm i\alpha \notin M$.

(v) Every finite, separable field extension is simple.
Solution: [B] True.

(vi) With t an indeterminate, $\mathbb{F}_3[t]/(t^2 + t + 1)$ is a field with 9 elements.
Solution: [P] False. Over $\mathbb{F}_3$, $t^2 + t + 1$ is not irreducible as 1 is a root. Hence $\mathbb{F}_3[t]/(t^2 + t + 1)$ is not a field.

(vii) The polynomial t^5+3 is separable over $\mathbb{F}_{25}$.
Solution: [U] True. $[(t+3)^5 = t^5+3^5 = t^5+3$ since 3 is in the prime subfield, which is fixed pointwiese by the Frobenius map. So the only irreducible factor of t^5+3 is $t+3$.]

(viii) $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$.
Solution [B] False. $\mathbb{C}$ contains elements, such as π and e, that are not algebraic over $\mathbb{Q}$, so $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$.

(ix) Suppose that $L : K$ is a field extension with $\gamma \in L$ so that γ is transcendental over K. Then $\gamma^3+\gamma+1$ is transcendental over $K(\gamma)$.
Solution: [P] False. $\gamma^3+\gamma+1 \in K(\gamma)$ (so $\gamma^3+\gamma+1$ is a root of $t-\gamma^3+\gamma+1$).

(x) Suppose that $t^n-\alpha \in \mathbb{Q}[t]$ and that $L : \mathbb{Q}$ is a splitting field extension for $t^n-\alpha$. Then L contains a primitive nth root of unity.
Solution: [B] False. Suppose that $n \geq 3$ and $\alpha = 0$; for instance, with $n = 4$, t^4 splits over $\mathbb{Q}$, but $\mathbb{Q}$ does not contain a primitive 4th root of unity.

(xi) There is a finite field L with subfields K_1, K_2 so that $[L : K_1] = [L : K_2]$ but K_1 is not isomorphic to K_2.
Solution: [B/P] False. Suppose that $|L| = p^r$ for some prime p, and $d = [L : K_1] = [L : K_2]$. Thus $|K_1| = p^{n/d} = |K_2|$ and hence $K_1 \simeq K_2$.

(xii) Suppose that $L : K$ is a splitting field extension for $f \in K[t] \setminus K$. If $\alpha \in L$ then $m_\alpha(K)$ splits in $L[t]$.
Solution: [B] True.

(xiii) With K a field, there are normal field extensions $L : K$ and $M : K$ with $K \subseteq L, M \subseteq \overline{K}$ and $(L \cap M) : K$ not a normal extension.
Solution: [P] False. If $\alpha \in L \cap M$, then all the roots of $m_\alpha(K)$ lie in L and lie in M, hence all these roots lie in $L \cap M$.

(xiv) With K a field and $f \in K[t] \setminus K$, if f has one multiple root in $\overline{K}$ then all the roots of f are multiple roots.
Solution: [P] False [although this is true if f is irreducible]. Suppose that $K = \mathbb{F}_3$ and $f = (t^3-1)(t-2)$. Then $f = (t-1)^3(t-2)$, so 1 is a multiple root of f but 2 is not.

(xv) Suppose that $L : M : K$ is a tower of field extensions so that $L : K$ is a normal extension. Then $L : M$ is a normal extension.
Solution: [B] True.

4. (a) **(5+3+4=12 marks)** Set $f = (t^2-5)(t^2+3)$, and let $L : \mathbb{Q}$ be a splitting field extension for f with $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$.

(i) Determine the degree of $L : \mathbb{Q}$, carefully justifying your answer.
Solution: [P] The roots of f are $\pm\sqrt{5}$, $\pm i\sqrt{3}$. So $L = \mathbb{Q}(\sqrt{5}, i\sqrt{3})$. By Eisenstein's criterion (with prime $p = 5$ and $p = 3$), both t^2-5 and t^2+3 are irreducible over $\mathbb{Q}$. So $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. We have $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$, and $i\sqrt{3} \notin \mathbb{R}$. Thus $\deg m_{i\sqrt{3}}(\mathbb{Q}(\sqrt{5})) > 1$. Also, since $i\sqrt{3}$ is a root of t^2+3, we know that $m_{i\sqrt{3}}(\mathbb{Q}(\sqrt{5}))$ divides t^2+3. Hence we must have $m_{i\sqrt{3}}(\mathbb{Q}(\sqrt{5})) = t^2+3$, and so $[L : \mathbb{Q}(\sqrt{5})] = 2$. Thus $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4$.

(ii) Describe the Galois group $Gal(L : \mathbb{Q})$ (that is, give generators and relations for the Galois group).
Solution: [P] Let $\tau, \sigma : L \to L$ be the homomorphisms so that $\tau(\sqrt{5}) = -\sqrt{5}$, $\tau(i\sqrt{3}) = i\sqrt{3}$, and $\sigma(\sqrt{5}) = \sqrt{5}$, $\sigma(i\sqrt{3}) = -i\sqrt{3}$. So

$$Gal(L : \mathbb{Q}) = \langle \tau, \sigma : \ \tau^2 = \sigma^2 = 1, \ \tau\sigma = \sigma\tau \ \rangle.$$

(iii) [P] Apply the Fundamental Theorem of Galois Theory to find all fields M for which $\mathbb{Q} \subsetneq M \subsetneq L$, explaining carefully how you applied the Fundamental Theorem in this process.
Solution: Each intermediate field M with $\mathbb{Q} \subsetneq M \subsetneq L$ corresponds to a subgroup H of $G = Gal(L : \mathbb{Q})$ with $\langle 1 \rangle \subsetneq H \subsetneq G$. The proper, nontrivial subgroup of G are $\langle \tau \rangle$, $\langle \sigma \rangle$, $\langle \tau\sigma \rangle$. We have $Fix_L\langle \tau \rangle = \mathbb{Q}(i\sqrt{3})$, $Fix_L\langle \sigma \rangle = \mathbb{Q}(\sqrt{5})$, and $Fix_L(\tau\sigma) = \mathbb{Q}(i\sqrt{15})$.

(b) **(7 marks)** Let $g = (t^2 - 2)(t^3 - 7)$, and let $L : \mathbb{Q}$ be a splitting field extension for g with $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$. Determine the value of $[L : \mathbb{Q}]$, carefully explaining your reasoning.
Solution: [U] The roots of g are $\pm\sqrt{2}, \alpha, \alpha\zeta, \alpha\zeta^2$ where $\alpha = \sqrt[3]{7} \in \mathbb{R}$ and $\zeta \in \mathbb{C}$ is a primitive 3rd root of unity (so $\zeta = e^{2\pi i/3}$ or $e^{4\pi i/3}$). As $t^2 - 2$, $t^3 - 7$ are irreducible over $\mathbb{Q}$ (by Eisenstein's criterion), we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Thus by the Tower Law, 2 and 3 divide $[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}]$. We also have that $m_\alpha(\mathbb{Q}(\sqrt{2})|m_\alpha(\mathbb{Q})$, so $\deg m_\alpha(\mathbb{Q}(\sqrt{2})) \leq 3$ and hence $[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}(\sqrt{2})] \leq 3$. Thus we have 6 dividing $[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}]$, and

$$[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}(\sqrt{2})] \cdot 2 \leq 6.$$

So we must have $[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}(\sqrt{2})] = 3$.
We have $\mathbb{Q}(\sqrt{2}, \alpha) \subseteq \mathbb{R}$, and $\zeta \notin \mathbb{R}$, which means that $\deg m_\zeta(\mathbb{Q}(\sqrt{2}, \alpha)) > 1$. As ζ is a root of $\frac{t^3-1}{t-1} = t^2 + t + 1$, we must have $m_\zeta(\mathbb{Q}(\sqrt{2}, \alpha)) = t^2 + t + 1$. Hence $[L : \mathbb{Q}(\sqrt{2}, \alpha)] = 2$. So by the Tower Law, $[L : \mathbb{Q}] = 12$.

(c) **(6 marks)**
Suppose that $E : \mathbb{Q}$ and $F : \mathbb{Q}$ are finite, normal extensions, with $\mathbb{Q} \subseteq E \subseteq \mathbb{C}$ and $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$. Also suppose that $\varphi : E \to F$ is an isomorphism. Show that $E = F$.
Solution: [U] Since $E : \mathbb{Q}$ and $F : \mathbb{Q}$ are finite normal extensions, there are $g, h \in \mathbb{Q}[t]$ so that $E : \mathbb{Q}$ is a splitting field extension for g and $F : \mathbb{Q}$ is a splitting field extension for h. We know that φ is a $\mathbb{Q}$-homomorphism since $\varphi(1) = 1$ and consequently φ is the identity map on $\mathbb{Q}$. So $\varphi(g) = g$, and thus with $\alpha_1, \ldots, \alpha_n$ the roots of g, we have that $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ are also roots of g, lying in F. As φ is necessarily one-to-one, $\{\alpha_1, \ldots, \alpha_n\} = \{\varphi(\alpha_1), \ldots, \varphi(\alpha_n)\}$. Hence $E \subseteq F$.
Similarly, with $\beta_1, \ldots, \beta_m$ the roots of h, $\varphi^{-1}(\beta_1), \ldots, \varphi^{-1}(\beta_m)$ are roots of h, and lie in E. So $F \subseteq E$.
Thus $E = F$.