

All questions may be attempted but only marks obtained on the best **four** solutions will count.

The use of an electronic calculator is **not** permitted in this examination.

1. (a) Let $L : K$ be a field extension and $\beta \in L$ with minimum polynomial m over K of degree n . Show that every element of $K(\beta)$ can be written uniquely as $g(\beta)$, where g is a polynomial over K of degree strictly less than n . Deduce that $[K(\beta) : K] = n$.
(b) State (do not prove) the Tower Law. Justifying your answers, find the following:
 - (i) $[\mathbf{Q}(\alpha^4 + 3\alpha^2 + 2) : \mathbf{Q}]$, where $\alpha = \sqrt[7]{5}$,
 - (ii) $[\mathbf{Q}(\sqrt[3]{1 + \sqrt{p}}) : \mathbf{Q}]$, where p is a prime congruent to 3 (mod 4).
2. (a) Prove Dedekind's Lemma (that any set of distinct monomorphisms from a field K to a field L are linearly independent over L).
(b) What does it mean to say that a group G is *soluble*? Show that the dihedral group $D_n = \langle x, y : x^n = y^2 = e, yx = x^{-1}y \rangle$ is soluble. Prove that if G is soluble, and H is a subgroup of G , then H is also soluble.
3. (a) Let $L : K$ be a field extension. Define what it means to say that $L : K$ is (i) *normal*, (ii) a *splitting field* for some polynomial f over K . Prove that if $L : K$ is a splitting field for some polynomial over K then $L : K$ is a normal extension.
(b) Determine whether each of the following extensions is normal or not, justifying your answers:
 - (i) $\mathbf{C}(t) : \mathbf{C}(t^3)$,
 - (ii) $\mathbf{C}(t) : \mathbf{C}(t^3 + t + 1)$.
4. Suppose that $L : \mathbf{Q}$ is a finite field extension.
 - (a) Stating clearly any results that you use, prove that there are only a finite number of fields M such that $\mathbf{Q} \subseteq M \subseteq L$.
 - (b) Hence prove that any finite extension of \mathbf{Q} is simple.
 - (c) Let $L = \mathbf{Q}(\sqrt{2}, \sqrt[5]{3})$. Find an element $\alpha \in L$ such that $L = \mathbf{Q}(\alpha)$, justifying your answer.

5. Let L be the splitting field of the polynomial $t^{11} - 1$ over \mathbf{Q} . Find the Galois group G of $L : \mathbf{Q}$. Find all intermediate fields K , i.e. fields K such that $\mathbf{Q} \subseteq K \subseteq L$, expressing them as simple extensions of \mathbf{Q} .

[You should justify your reasoning but may assume relevant results, including the Fundamental Theorem of Galois Theory.]