All fields are taken to be subfields of the complex numbers $\mathbb{C}$. You may assume results from group theory.

1. Let E/F be a finite extension of fields. Define the *degree* $|E : F|$ of E over F.

   State and prove the *Tower Law* for a chain $F \subset K \subset E$ of fields.

   Suppose that $|E : F| = mn$ where m, n are coprime integers, and that there are intermediate fields K, L with $|K : F| = m$, $|L : F| = n$. Prove that E is the smallest field that contains both K and L, and find $|E : K|$ and $|E : L|$.

   Let $f(X)$ and $g(X)$ be irreducible polynomials over F, of coprime degrees m, n respectively, and let M be a splitting field for $f(X)g(X)$. Show that mn divides $|M : F|$.

   Give, without proofs, examples of polynomials over $F = \mathbb{Q}$, where

   (1) $mn = |M : F|$;

   (2) $mn < |M : F|$.

2. Define the *Galois group* $G = \mathrm{Gal}(E/F)$ of a finite normal extension E/F of fields.

   Given an intermediate field K, define the subgroup K^* of G.

   Given a subgroup H of G, define the intermediate field $H^\dagger$.

   State the relationship between K and $K^{*\dagger}$, and between $H^{\dagger *}$ and H.

   Show that K/F is normal if and only if $H = K^*$ is a normal subgroup of G.

   Given that K/F is normal, find its Galois group.

3. Let $\alpha = \sqrt{2 + \sqrt{3}}$. Find the minimal polynomial $p(X)$ of α over $\mathbb{Q}$, and find the conjugates of α. Show that they can be arranged in pairs $\{\alpha_i, \beta_i\}$ so that $\alpha_i \beta_i = 1$ for each i.

   Prove that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a normal extension, find $\mathrm{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q})$ and describe all the intermediate fields in the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$.

   Now put $\gamma = \sqrt{1 + \sqrt{3}}$. Find the minimal polynomial $q(X)$ of γ over $\mathbb{Q}$, and explain why $\mathbb{Q}(\gamma)$ is *not* the splitting field of $q(X)$. Describe the splitting field of $q(X)$.

4. Let $f(X) = X^p - 2$, where p is prime. Show that if $f(X)$ splits in a field L, then L must contain a primitive p-th root ω of unity. Hence find the splitting field E of $f(X)$.

Show that $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is cyclic of order $p-1$ – you may assume that the corresponding cyclotomic polynomial is irreducible, and that the multiplicative group $\mathbb{Z}_p^*$ is cyclic.

Hence find $\mathrm{Gal}(E : \mathbb{Q})$, giving two generators and the relation between them.

5. Let $f(X)$ be a monic polynomial over $\mathbb{Q}$. Say what is meant by *'f(X) can be solved by radicals'*.

Let $E/\mathbb{Q}$ be a normal extension with Galois group $G = \mathrm{Gal}(E : F)$. Let L/E be an extension of fields and suppose there is a tower $\mathbb{Q} \subset N \subset M \subset L$ with M/N normal of prime degree q. Show that the extension $M \cap E/N \cap E$ is either trivial or normal of prime degree.

Outline briefly the remaining steps required to show that, if $f(X)$ is solvable by radicals, then G is a solvable group.