1. Suppose that K is a field of characteristic zero, and $p(x) \in K[x]$ an irreducible polynomial of degree d over K. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the roots of $p(x)$, and $L = K(\alpha_1, \ldots, \alpha_d)$ the field obtained by adjoining all the roots of $p(x)$.

Let S be the set $S = \{\alpha_1, \ldots, \alpha_d\}$ of the roots.

(a) If σ is an element of $\mathrm{Aut}(L/K)$ explain why, for any root $\alpha_i \in S$, $\sigma(\alpha_i) \in S$ too, so that the group $G = \mathrm{Aut}(L/K)$ acts on the set S.

(b) If $\sigma \in G$, and $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, d$, explain why σ is actually the identity map $\sigma : L \longrightarrow L$ on L.

(c) An action of a group G on a set S is the same as a homomorphism $G \longrightarrow \mathrm{Perm}(S)$ from G to the group of permutations of S. Explain why the action from part (a) gives an *injective* homomorphism.

(d) Explain why the group G acts *transitively* on S.

(e) Explain why the group G above can be realized as a subgroup of S_d, the symmetric group on d elements, such that the subgroup acts transitively on the set $\{1, \ldots, d\}$.

2. Let $K = \mathbb{Q}$, and $\alpha = e^{2\pi i/7}$. The minimal polynomial for α over $\mathbb{Q}$ is $q(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

(a) Show that $L = \mathbb{Q}(\alpha)$ is a/the splitting field for $q(x)$.

(b) If $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$, show that σ is completely determined by what it does to α. (i.e., once you know what $\sigma(\alpha)$ is, you know how σ acts on all of L.)

(c) Compute the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. (Keeping in mind parts (d) and (e) of question 1 may help, but don't get hung up on it if it doesn't.)

(d) Describe the subgroups of G, and draw the corresponding diagram of intermediate fields between $\mathbb{Q}$ and L.

3. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[4]{3}, i)$.

(a) Is L/K a Galois extension?

(b) Explain carefully (by following through the steps of the lifting lemma) how you know there is an automorphism $\sigma \in \mathrm{Aut}(L/K)$ with $\sigma(\sqrt[4]{3}) = \sqrt[4]{3}i$. Is there such a σ with $\sigma(\sqrt[4]{3}) = \sqrt[4]{3}i$ and $\sigma(i) = i$? What is the group $G = \mathrm{Aut}(L/K)$ in this case?

(c) Which subgroup H of G corresponds to the intermediate field $\mathbb{Q}(\sqrt[4]{3})$?

(d) What are the subgroups H' of G containing H? Which intermediate fields to they correspond to?

(e) What are the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{3})$?

4. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[4]{3}, i)$ as in question 3. Suppose that (α_1, β_1), $\dots$, (α_k, β_k) are pairs of numbers in L, and that the set $S = \{(\alpha_1, \beta_1), \dots, (\alpha_k, \beta_k)\}$ is stable under the action of $G = \mathrm{Aut}(L/K)$. (This means that if $(\alpha_i, \beta_i) \in S$ then $(\sigma(\alpha_i), \sigma(\beta_i)) \in S$ for any $\sigma \in G$). For any $d \geq 0$, consider the L-vector space V_d of polynomials of degree $\leq d$ in $L[x, y]$ which are zero at all (α_i, β_i), $i = 1, \dots, k$. Show that V_d has a basis consisting of polynomials with coefficients in $\mathbb{Q}$.

PUZZLE: If the questions above are too straightforward, you may want to try this optional question.

Suppose we start with $L = \mathbb{Q}(i) = \left\{ a + bi \;\middle|\; a, b \in \mathbb{Q} \right\}$, considered as a vector space of dimension 2 over $\mathbb{Q}$. Let $\alpha = i \in L$. Multiplication by α is a linear map from L to L, and so we can write out a matrix for this linear transformation. If we use the standard basis $\{1, i\}$ for L over $\mathbb{Q}$, the matrix is

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

The characteristic polynomial for this matrix is $\lambda^2 + 1$, so we see that this matrix has eigenvalues i and $-i$. The puzzle is this: Where did the $-i$ come from? Shouldn't multiplication by i just have i as its only eigenvalue (but repeated twice)? (For instance, over any real vector space, the linear transformation "multiplication by 2" has matrix 2 times the identity, and all eigenvalues are 2).

You may also want to look at the field $L = \mathbb{Q}(\sqrt[3]{2})$, and what happens if you multiply by $\alpha = \sqrt[3]{2}$.

A successful resolution of this puzzle is a general statement about what the eigenvalues of "multiplication by α" are in a field L, considered as a vector space over a finite-dimensional subfield K, as well as an argument why this is correct.