Problem 1

Let F be a field of prime characteristic p. Suppose $E = F(\alpha)$ such that $\alpha \notin F$ but $\alpha^p - \alpha \in F$.

1. Find $[E : F]$.

2. Prove that E/F is a Galois extension.

3. Find the Galois group $\text{Gal}(E/F)$.
   Hint: Note that $(x + 1)^p - (x + 1) = x^p - x$.

Proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Problem 2

Let $\zeta := e^{2\pi i/7}$ be a primitive 7th root of unity. Let $K = \mathbb{Q}(\zeta)$.

1. Prove that there exists an element $\alpha \in K$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

2. Express α in terms of ζ.

Proof. We will prove two items at once. Consider the element given by

$$\alpha = \zeta + \zeta^2 + \zeta^4$$

Then it can be seen that the map σ such that σ such that $\sigma(\zeta) = \zeta^3$ generates the Galois group of the cyclotomic field. This implies the desired field extension will correspond to the fixed field of the subgroup generated by σ^2. We can see that the α defined as above is fixed by $\theta = \sigma^2$. Indeed

$$\theta(\alpha) = \sigma^2(\zeta + \zeta^2 + \zeta^4) = \zeta^9 + \zeta^4 + \zeta^{36} = \zeta^2 + \zeta^4 + \zeta = \alpha$$

Clearly $\alpha \notin \mathbb{Q}$, since ζ has degree 6 over $\mathbb{Q}$. Moreover, α can't have degree 3 over $\mathbb{Q}$, otherwise it is inside the intersection of two intermediate fields of degree 2 and 3, thus is rational. Hence we can conclude that this is the desired element. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Remark: A sage code for this problem is given below.

```
k = CyclotomicField(7); k
zeta=k.gen(); a = zeta+zeta^2+zeta^4
a.minpoly()
```