M622 Final-like problems
These are all important.

1. Let $n \in \mathbb{N}$, $n > 1$, F contains the nth roots of unity, $a \in F$, and $K = F(a^{1/n})$ is contained in $\mathbb{C}$.
   (a) Show that K is a splitting field of some polynomial $t(x) \in F[x]$: What is $t(x)$?
   (b) Show that there exists an injection $\iota : Gal(K/F) \to Z_n$.
   (c) Explain why $Gal(K/F)$ is cyclic, and why $[K : F] \mid n$.

2. Suppose K/F is a field extension, F is infinite, but there are only finitely many intermediate fields $\{J : F \leq J \leq K\}$. Prove that there exists $\theta \in K$ such that $K = F(\theta)$.

3. Let F be a finite field of characteristic p, where p is a prime number.
   (a) Explain why there exists $n \in \mathbb{N}$ such that $|F| = p^n$. (Suggestion: Use that any field of characteristic p has as its prime subfield $\mathbb{F}_p$, the field with p elements. Then explain that F is a vector space over $\mathbb{F}_p$ etc.)
   (b) If $|F| = p^n$, show that F is the splitting field of $t(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. (A start: $p^n - 1 = |F^x|$, the multiplicative group on $F - \{0\}$, so if γ is not 0, by a corollary of Lagrange, $\gamma^{p^n-1} = 1$. So $\gamma^{p^n} - \gamma = 0$.)
   (c) Recall the following:
      i. (*) If $t(x) \in \mathbb{F}_p[x]$ has degree n, then $t(x)$ has at most n roots in any extension field of F.
      ii. (**) Let H be a finite group. It follows from a corollary of Lagrange's Theorem that for all $g \in H$, $g^{|H|} = e$. Recall that the *exponent* of H is $\min\{k \in \mathbb{N} : \forall g \in H\ g^k = e\}$. It follows that the exponent of H is no greater than $|H|$. We proved that (***) if H is finite Abelian, then H is cyclic if and only if the exponent of H is $|H|$. (A note in passing: There are finite non-Abelian groups G such the exponent of G is $|G|$, but G is not cyclic.)
   (d) Use (*) and (***) above to show that F^x is cyclic.

4. Let F be a finite field with p^n elements, p a prime, $n \in \mathbb{N}$. The Froebenius map $\phi : F \to F$ such that $\phi(\gamma) = \gamma^p$ for all $\gamma \in F$ is an

automorphism of F, and is in $Aut(F/\mathbb{F}_p$. F is Galois over $\mathbb{F}_p$—as you showed, F is a splitting field of $t(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Give a clear well-reasoned showing $Aut(F/\mathbb{F}_p)$ is cyclic.

5. Prove that if G is an Abelian simple group, then there exists a prime p such that $G \cong Z_p$, the p-element additive group. Then use this fact to show the following:

   (a) If G is an infinite Abelian group, then G has no composition series.

   (b) Recall a finite group H is solvable if it has a composition series having cyclic factors. Prove that if G is a finite Abelian group, then G is solvable. (I suggest doing it by induction on $|G|$.

   (c) Prove that if G is a finite group and N is normal in G, then there exists a composition series of G that has N in it.

   (d) Use the above to show that if G is a finite solvable group, and N is a normal subgroup of G, then G/N is solvable. (You'll use the Fourth Isomorphism Theorem—a.k.a. the Correspondence Theorem—and then the Third Isomorphism Theorem.)

6. Suppose F is a field and K and L are both extensions of F. Recall that "LK" is the least field that contains L and K. Assume that LK exists, and show that if $([K : F], [L : F]) = 1$, then $[LK : F] = [K : F][L : F]$. (Suggestion: You could first show that $[K : F][L : F] \geq [KL : F]$, and go from there.)

   Then show, by an example, that if $([K; F], [L : F]) > 1$, it is possible that $[LK : F]$ is smaller than $[K : F][L : F]$.