Midterm Exam

Problem 1. Let p be a prime number, $m \geq 1$, and $q := p^m$. Let $\ell \geq 1$.

(1) Recall the definition of the Frobenius of a field K with characteristic p and recall why it is a morphism of fields.
(2) Show that the field $\mathbb{F}_q$ is perfect.
(3) What is the degree of the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$? Justify.
(4) Show that the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ is Galois.
(5) Recall what is the Galois group of $\mathbb{F}_{q^\ell}/\mathbb{F}_q$. (You don't need to give the proof of this).

Problem 2. Let k be a field and $P \in k[X]$ with degree $n \geq 1$.

(1) Suppose in this question that P is irreducible.
   (a) Recall the definition of the stem field F of P.
   (b) Let K be an extension of k. Show that if K contains a root of P then K is an extension of F.
(2) Show that if P is reducible, then there is an extension E/k with degree $\leq n/2$ containing a root for P.
(3) Let p be a prime number and suppose that $k = \mathbb{F}_p$.
   (a) Show that P is irreducible if and only if P has no root in $\mathbb{F}_{p^d}$ for all $d \leq n/2$.
   (b) Show that P is irreducible if and only if $\mathrm{GCD}(P, X^{p^d} - X) = 1$ for any $1 \leq d \leq n/2$.

Problem 3. We admit the following theorem :

Theorem (Artin's Lemma)**.** Let E be a perfect field and G a finite subgroup of the group of automorphisms of the field E. Then the field $E_0 := \{x \in E,\ gx = x \text{ for any } g \in G\}$ is perfect and E/E_0 is a finite Galois extension with Galois group G.

Let $n \geq 1$. Recall that $\mathfrak{S}_n$ denotes the permutation group of a set with n elements. Consider the ring of polynomials with n variables $\mathbb{Q}[X_1, ..., X_n]$ and $\mathbb{Q}(X_1, ..., X_n)$ its fraction field.

(1) Show that $\mathfrak{S}_n$ can be seen as a subgroup of the group of automorphisms of the field $\mathbb{Q}(X_1, ..., X_n)$
(2) Let G be a group with n elements.
   (a) Find an injective morphism of groups $G \to \mathfrak{S}_n$.
   (b) Use Artin's lemma to find a Galois extension with Galois group G.

Problem 4 (Optional)**.** Let $n \geq 1$ and ζ_n be a primitive n^{th}-root of 1 in $\mathbb{C}$. Show that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois and that there is an injective morphism of groups

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

This proves in particular that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian.