Before you start, please read the syllabus carefully.

1. Let $F$ be an arbitrary field with $\text{char}(F) = p$. Prove that $F_p \subset F$, i.e., $F_p$ is a subfield of $F$. (This is a quick proof of $F_p \subset S$ of Claim 2 in class.)

2. Prove that for an irreducible polynomial $f(x) \in F_p[x]$, the field extension $F_p[x]/\langle f(x) \rangle$ is also the splitting field of $f(x)$. (Hint: prove that $f(x)|x^q - x$ for $q = p^{\text{deg}(f)}$.)

3. Prove that $F_p^d$ is a subfield of $F_p^n$ if and only if $d|n$.

4. For an arbitrary field $F$, we define a formal operation on $f(x) \in F[x]$ called derivative as following

$$f'(x) := \sum_n a_n \cdot n \cdot x^{n-1},$$

if $f(x) = \sum_n a_n \cdot x^n$.

(a) Prove that

$$\left( f(x) \cdot g(x) \right)' = f'(x) \cdot g(x) + f(x) \cdot g'(x),$$

for $F[x]$ for arbitrary field $F$.

(b) Prove that if $f(x)$ has a multiple root $\alpha$, equivalently $(x - \alpha)^2|f(x))$, then $\alpha$ is also a root of $f'(x)$.

(c) Does the converse from above holds? i.e., if $f'(\alpha) = 0$, does it imply that $\alpha$ is a multiple root $f(x)$? If yes, give a proof, if no, give a counter example or give a correct statement.

(d) Prove that $f(\alpha) = f'(\alpha) = \cdots = f^{(k)}(\alpha) = 0$ if and only if $(x - \alpha)^{k+1}|f(x)$ for $f(x)$ in polynomial ring $F[x]$ where $F$ is an arbitrary field. (Does this remind you of Taylor expansion in calculus?)

5. Let $f(x) = x^2 + x + 1 \in F_p[x]$ where $p > 3$ is a prime number.

(a) Determine if $f(x)$ is irreducible in $F_p[x]$. (Give a criteria on when $f(x)$ is irreducible.)

(b) For $p = 5$, using your criteria to determine whether $f(x)$ is irreducible. If yes, denote $K = F_5[x]/\langle f(x) \rangle$. Show that $K$ contains all 24-th roots of unity $\zeta_{24}$ (i.e. elements $\alpha$ such that $\alpha^{24} = 1$).

(c) For $p = 7$, using your criteria to determine whether $f(x)$ is irreducible. If no, determine the factorization of $f(x)$.

(d) The largest prime number ever found up to now is $p = 2^{82589933} - 1$. Use your criteria to determine whether $f(x)$ is irreducible. You are not allowed to use computer.
6. Let \( f_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{F}_3[x] \) where \( p > 3 \) is a prime number. Denote \( K_p \) to be the splitting field of \( f_p(x) \) over \( \mathbb{F}_3 \).

(a) Prove that \( x^r - 1 \mid x^s - 1 \) in \( \mathbb{F}_3[x] \) if and only if \( r \mid s \).

(b) Prove that \( f_p(x) \mid x^q - x \) for \( q = 3^n \) if and only if \( p \mid 3^n - 1 \).

(c) Determine \( [K_p : \mathbb{F}_3] \).

(d) Determine when \( f_p(x) \) is irreducible in \( \mathbb{F}_3[x] \). For \( p = 7, 11, 13 \), use your criteria to determine yes/no.

7. Given \( \sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q \) such that \( \sigma(x) = x^p \). Prove that \( \sigma \) is a ring isomorphism.