Let $\Phi_n(x)$ be the $n$th cyclotomic polynomial. Suppose $p$ is an odd prime which does not divide $n$. Let $\Phi_{n,p}(x) \in \mathbb{F}_p[x]$ be $\Phi_n(x)$ modulo $p$. Let $E \subseteq \overline{\mathbb{F}}_p$ be a splitting field of $\Phi_{n,p}(x)$ over $\overline{\mathbb{F}}_p$.

1. Prove that $x^n - 1$ does not have multiple zeros in $\overline{\mathbb{F}}_p$.

2. Suppose $\zeta \in E$ is a zero of $\Phi_{n,p}(x)$. Prove that $\zeta$ is not a zero of $\Phi_{d,p}(x)$ for $d \mid n$ and $d \neq n$. Deduce that $o(\zeta) = n$ as an element of $E^\times$.

3. Use part (2), to show $\Phi_{n,p}(x) = \prod_{1 \leq i \leq n, \gcd(i,n)=1} (x - \zeta_i)$. Deduce that $E = \mathbb{F}_p[\zeta]$, and $\text{Gal}(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Use the fact that the Frob. map $x \mapsto x^p$ generates $\text{Gal}(\mathbb{F}_p[\zeta]/\mathbb{F}_p)$ to deduce $\text{Gal}(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \cong \langle p \rangle$, where $\langle p \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$.

4. Prove, if $\Phi_{n,p}(x)$ has a zero in $\mathbb{F}_p$, then $n \mid p-1$.

Use this to show there are infinitely many primes of the form $\frac{p^k-1}{p-1}$.
(5) Prove that $\Phi_n(p) \in \mathbb{F}_p[x]$ is irreducible $\iff <p> = (\mathbb{Z}/n\mathbb{Z})^x$.

2. Suppose $\mathbb{Q}[\zeta_n] \subseteq \mathbb{F} \subseteq \mathbb{C}$ is a tower of fields where $\zeta_n = e^{2\pi i/n}$.
   
   (a) For $a_1, a_2 \in \mathbb{F}^x$, prove that
   
   $$\mathbb{F}[\sqrt[n]{a_1}] = \mathbb{F}[\sqrt[n]{a_2}] \iff a_1(\mathbb{F}^x)^n = a_2(\mathbb{F}^x)^n$$
   
   (Here $\sqrt[n]{a}$ means an element of $\mathbb{C}$ which is a zero of $x^n - a$.)
   
   (b) Prove that $\mathbb{F}[\sqrt[n]{a}] / \mathbb{F}$ is a Galois extension for any $a \in \mathbb{F}^x$, and $\text{Gal}(\mathbb{F}[\sqrt[n]{a}] / \mathbb{F}) \cong <a(\mathbb{F}^x)^n> \subseteq \mathbb{F}^x / (\mathbb{F}^x)^n$.

3. Suppose $E / F$ is a finite extension. For any $a \in E$, let $l_a : E \to E$, $l_a(e) = ae$. View $l_a$ as an element of $\text{End}_F(E)$.
   
   Prove that $E / F$ is separable if and only if $\forall a \in E$, $l_a$ is diagonalizable over an algebraic closure $\overline{F}$ of $F$.

4. Let $F$ be a field. Suppose for any finite extension $E / F$, $p \mid [E : F]$, where $p$ is an odd prime.
   
   (a) Suppose $E / F$ is a finite separable extension. Prove $[E : F] = p^n$ for some $n \in \mathbb{Z}^{>0}$.
   
   (b) Suppose $F$ is not perfect. Prove $\text{char}(F) = p$.
   
   (c) Suppose $E / F$ is any finite extension. Prove $[E : F] = p^n$. 
5. Suppose \( E/F \) is an algebraic extension. Let

\[
F^{ab} := \{ x \in E \mid F[x]/F \text{ is Galois and } \text{Gal}(F[x]/F) \text{ is abelian} \}
\]

(a) Suppose \( F \subseteq K \subseteq E \), \( K/F \) is Galois, and \( \text{Gal}(K/F) \) is abelian. Prove that \( K \subseteq F^{ab} \).

(b) Prove that \( F^{ab} \) is a field.

(c) Prove that \( F^{ab}/F \) is Galois and \( \text{Gal}(F^{ab}/F) \) is abelian.

6. Let \( q = p^n \) where \( p \) is a prime and \( n \in \mathbb{Z}^+ \). Prove that any irreducible factor of \( x^q - x + 1 \in \mathbb{F}_q[x] \) has degree \( p \).

(Hint: Suppose \( \alpha \) is a zero of \( x^q - x + 1 \) in a splitting field. Prove that \( \alpha^{q^i} = \alpha - i \); and so \( \alpha^p = \alpha \) and \( \alpha^i \neq \alpha \) for \( 1 \leq i \leq p-1 \).

Hence \( \mathbb{F}_q[\alpha] = \mathbb{F}_{q^p} \).)

7. Suppose \( F \) is a field, \( f(x) \in F[x] \) is irreducible, and \( E \) is a splitting field of \( f(x) \) over \( F \). Suppose \( \exists \alpha \in E \) s.t. \( f(\alpha) = f(\alpha + 1) = 0 \). Prove that

(a) \( \text{Char } F = p > 0 \).

(b) \( \exists F \subseteq K \subseteq E \) s.t. \( E/K \) is Galois and \( [E:K] = p \).
Suppose \( F \) is a field and \( \text{char}(F) \neq 2 \). Let \( a_1, \ldots, a_n \in F^\times \),

\( H := \langle a_1(F^\times)^2, \ldots, a_n(F^\times)^2 \rangle \leq F^\times/(F^\times)^2 \), and \( E := F[\sqrt{a_1}, \ldots, \sqrt{a_n}] \).

1. Prove that \( E/F \) is a Galois extension.

2. Let \( G := \text{Gal}(E/F) \). Prove that \( G \) is an elementary abelian 2-group; that means \( G \cong (\mathbb{Z}/2\mathbb{Z})^m \) for some \( m \in \mathbb{Z}^+ \).

3. Prove that \( H \) is an elementary abelian 2-group.

4. Let \( T: G \times H \to \mathbb{Z}/2\mathbb{Z} \) be

\[
T(\sigma, a(F^\times)^2) := \sigma(\sqrt{a})/\sqrt{a}.
\]

Prove that \( T \) is a non-degenerate bilinear form; that means

\[
T(\sigma_1 \sigma_2, \overline{a}) = T(\sigma_1, \overline{a}) T(\sigma_2, \overline{a}),
\]

\[
T(\sigma, \overline{a} \overline{a'}) = T(\sigma, \overline{a}) T(\sigma, \overline{a'}), \text{ and}
\]

\[
\begin{cases}
\forall \sigma \in G, \quad T(\sigma, \overline{a}) = 1 \Rightarrow \overline{a} = \overline{1} \\
\forall \overline{a} \in H, \quad T(\overline{a}, \overline{a}) = 1 \Rightarrow \overline{a} = \text{id}_E
\end{cases}
\]

5. Deduce that \( \text{Gal}(F[\sqrt{a_1}, \ldots, \sqrt{a_n}]/F) \cong \langle a_1(F^\times)^2, \ldots, a_n(F^\times)^2 \rangle \).
10. In class we proved that \( \text{Aut}(\mathbb{F}/\mathbb{F}) \cong \varprojlim_{E/\mathbb{F}, \text{normal}} \text{Aut}(E/\mathbb{F}) \). And so

\[
\text{Aut}(\overline{\mathbb{F}}/\mathbb{F}) \cong \varprojlim_{n} \text{Aut}(\mathbb{F}_n/\mathbb{F}).
\]

Deduce that

\[
\text{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \cong \varprojlim_{n} \mathbb{Z}/n\mathbb{Z} := \langle a_m \rangle \in \text{Gal}(\mathbb{Z}/n\mathbb{Z}) \text{ s.t. } a_m \equiv a_0 \mod n.
\]

(2) Prove that \( \varprojlim_{n} \mathbb{Z}/n\mathbb{Z} \) has no non-trivial torsion element.

(3) Suppose \( E \subseteq \overline{\mathbb{F}} \) is a subfield and \( [\overline{\mathbb{F}}:E]<\infty \).

Prove that \( E = \overline{\mathbb{F}} \).

10. Suppose \( E/\mathbb{F} \) is a finite Galois extension. Suppose

\[
\text{Gal}(E/\mathbb{F}) = \langle \sigma \rangle.
\]

View \( \sigma \) as an element of \( \text{End}_\mathbb{F}(E) \).

Let \( n := [E:\mathbb{F}] \). For \( a \in E \), let \( \ell_a : E \to E, \ell_a(e) = ae \).

View \( \ell_a \) as an element of \( \text{End}_\mathbb{F}(E) \); and let \( \tau_a := \ell_a \circ \sigma \).

(1) Prove that \( \tau_a^i = \ell_a \circ \sigma \circ \cdots \circ \sigma \circ \sigma^i \).

(2) Prove that the minimal polynomial of \( \tau_a \) (as an element of \( \text{End}_\mathbb{F}(E) \)) is \( x^n - N_{E/\mathbb{F}}(a) \) where \( N_{E/\mathbb{F}}(a) = \prod_{i=0}^{n-1} \sigma^i(a) \).

(3) Find rational canonical form of \( \tau_a \).
(4) Suppose, for $a \in E^x$, $N_{E/F}(a) = 1$. Show $\tau_a$ has eigenvalue one, and deduce $\exists b \in E \text{ st. } a = b/\sigma(b)$. 

(5) Prove that $N_{E/F} : E^x \rightarrow F^x$ is a group homomorphism and 

$$\ker(N_{E/F}) = \langle \sigma(b) \mid b \in E^x \rangle.$$ 

(6) Prove $\exists \alpha \in E \text{ s.t. } \alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)$ is an $F$-basis of $E$. (Hint: Use part (3) for $a = 1$..)