1 Let $n \geq 3$ be an odd integer such that $\operatorname{char} F \nmid n$.

(a) Show that the cyclotomic polynomial $\Phi_n \in F[X]$ has even degree.

Proof. We perform (strong) induction on n.

For the base case $n = 3$, we have $\Phi_3 = X^2 + X + 1$, so $\deg \Phi_3 = 2$.

Assume that the result holds for all odd integers d with $3 \leq d < n$. We now write

$$X^n - 1 = \prod_{\substack{1 \leq d \leq n \\ d \mid n}} \Phi_d.$$

Because n is odd, then $d \mid n$ only if d is also odd, so we can write

$$X^n - 1 = \Phi_1 \Phi_n \prod_{\substack{3 \leq d < n \\ d \mid n}} \Phi_d.$$

Then taking degrees, we obtain

$$\deg \Phi_n = \deg(X^n - 1) - \deg \Phi_1 - \sum_{\substack{3 \leq d < n \\ d \mid n}} \deg \Phi_d = n - 1 - \sum_{\substack{3 \leq d < n \\ d \mid n}} \deg \Phi_d.$$

By the inductive hypothesis, each $\deg \Phi_d$ is even. And since $n - 1$ is also even, this equation tells us that $\deg \Phi_n$ is even. □

(b) Now assume that $\operatorname{char} F \nmid 2n$. Show that $\Phi_{2n} = \Phi_n(-X)$. [Hint: Show that in an algebraic closure $\overline{F}$ of F, the primitive $2n$th roots of unity are exactly the elements $-\zeta$ where ζ is a primitive nth root of unity in $\overline{F}$.]

Proof. Per the hint, fix an algebraic closure $\overline{F}$ of F.

Suppose $\zeta \in \overline{F}$ is a primitive nth root of unity. Then

$$(-\zeta)^{2n} = ((-1)^2)^n (\zeta^n)^2 = 1^n \cdot 1^2 = 1,$$

so $-\zeta$ is a $2n$th root of unity. Because ζ is a primitive nth root of unity, we know that $\zeta^j \neq 1$ for $1 \leq j < n$. Moreover, since n is odd, we also know $\zeta^j \neq -1$ for $1 \leq j < n$, since -1 is the primitive 2nd root of unity. It follows that $\zeta^{n+j} = -\zeta^j \neq 1$ for $1 \leq j < n$, and we conclude that $-\zeta$ is a primitive $2n$th root of unity.

Use similar argument to show ζ primitive $2n$th root implies $-\zeta$ primitive nth root.

By definition, we have $\Phi_n = \prod (X - \zeta)$, where the product is taken over all $\zeta \in \overline{F}$ primitive nth roots of unity. Since the $-\zeta$'s are precisely the primitive $2n$th roots of unity, we deduce

$$\Phi_{2n} = \prod (X + \zeta) = \prod -(-X - \zeta) = (-1)^{\deg \Phi_n} \Phi_n(-X) = \Phi_n(-X).$$

□

2 Suppose $\operatorname{char} F = 0$, and let $f \in F[X]$ be irreducible. Moreover, assume there exists an extension by radicals $F \subseteq K$ such that f has a root in K. Show that f is solvable by radicals over F.

Proof. Let L be a normal closure of K over F, then Lemma 8.6 tells us that $F \subseteq L$ is an extension by radicals. Since $F \subseteq L$ is normal and $f \in F[X]$ is irreducible, we know that f must split over L. Hence, f is solvable by radicals over F. $\square$

3 Let $F \subseteq K$ be a Galois field extension with finite degree, such that $\mathrm{char}(F) \neq 2$. An *iterated square root extension of* F is any field L for which there exists a tower

$$L_0 = F \subseteq L_1 \subseteq \cdots \subseteq L_n = L$$

with $L_i = L_{i-1}(a_i)$ and $a_i^2 \in L_{i-1}$ for $1 \leq i \leq n$. Prove that the following conditions are equivalent:

(a) K is an iterated square root extension of F.

(b) K is contained in an iterated square root extension of F.

(c) $G(K : F)$ is a 2-group.

Proof. Assuming (a) is true, then (b) follows trivially since $K \subseteq K$.

Assume (b) is true—say K is contained in an iterated square root extension L of F. By repeatedly applying the tower rule to the tower in the definition of L, we obtain

$$[L : F] = [L_n : L_{n-1}] \cdots [L_1 : L_0].$$

To compute this degree, we consider each extension $L_i = L_{i-1}(a_i)$ in the tower. If $a_i \in L_{i-1}$ then $L_i = L_{i-1}$, so $[L_i : L_{i-1}] = 1$. If $a_i \notin L_{i-1}$ then the minimal polynomial of a_i over L_{i-1} is simply $X^2 - a_i^2$, so

$$[L_i : L_{i-1}] = \deg(X^2 - a_i^2) = 2.$$

Thus, $[L_i : L_{i-1}]$ is either 1 or 2 for all $i = 1, \ldots, n$. It follows that $[L : F]$ is a power of 2, i.e., $[L : F] = 2^m$ for some nonnegative integer m. Now apply the tower rule to $F \subseteq K \subseteq L$ to obtain

$$2^m = [L : F] = [L : K][K : F].$$

Hence, $[K : F]$ is also a power of 2, i.e., $G(K : F)$ is a 2-group.

Lastly, we prove (c) implies (a) by induction on m, where $[K : F] = |G(K : F)| = 2^m$.

For the base case, assume $[K : F] = 2$. Necessarily, we must have $K = F(b)$ where the minimal polynomial of b over F is a quadratic $X^2 + \beta X + \gamma \in F[X]$. Since $\mathrm{char}\, F \neq 2$, then we can also write $K = F(a)$ for $a = \beta + 2b \in K$. Then squaring a gives us

$$a^2 = (\beta + 2b)^2 = \beta^2 + 4(b^2 + b\beta) = \beta^2 - 4\gamma,$$

which is an element of F. In other words, K is a square root extension of F.

For the inductive step, assume the result holds for powers of 2 up to $m - 1$ for $m \geq 2$. (That is, we assume that whenever we have a Galois group of order 2^k with $1 \leq k \leq m - 1$, the corresponding fields form an iterated square root extension.) Recall that, by assumption, $G = G(K : F)$ is a group of order 2^m. We claim that there is a nontrivial proper normal subgroup of G. To see this, let G act on itself via conjugation and let $x_1, \ldots, x_r \in G$ be representatives of the non-center conjugacy classes, then the class equation gives us

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)],$$

where $Z(G)$ is the center of G and $C_G(x_i)$ is centralizer of x_i in G. Note that each $[G : C_G(x_i)]$ is a positive power of 2—say 2^{k_i} for $k_i \geq 1$. Then we write

$$2^m = |Z(G)| + \sum_{i=1}^{r} 2^{k_i}.$$

Since $Z(G)$ contains at least the identity, then $|Z(G)| \geq 1$, but in order for the above equation to hold we must in fact have $|Z(G)| > 1$. In other words, the center of G is nontrivial.

We may now choose $H \trianglelefteq G$ to be a nontrivial proper normal subgroup: if G is abelian then any nontrivial proper subgroup will do, otherwise we take the center of G. By the main theorem of Galois theory, the fixed field $L = \mathrm{Fix}_K(H)$ is a intermediate field $F \subseteq L \subseteq K$ with both extensions $F \subseteq L$ and $L \subseteq K$ nontrivial and Galois. By the tower rule,

$$2^m = [K : F] = [K : L][L : F],$$

which implies

$$|G(K : L)| = [K : L] = 2^k \quad \text{and} \quad |G(L : F)| = [L : F] = 2^\ell,$$

where $1 \leq k, \ell \leq m - 1$. By the inductive hypothesis, both $F \subseteq L$ and $L \subseteq K$ are iterated square root extensions. Joining their respective towers from the definition at L shows that $F \subseteq K$ is also an iterated square root extension. $\square$